Guardian Digital
Secure Mail Suite

User Guide

Copyright © 2004 Guardian Digital, Inc.

Contents

1 Introduction **1**

2 Contacting Guardian Digital **2**

3 Guardian Digital Master Support **3**

4 Installing Guardian Digital Secure Mail Suite **4**

4.1 Accessing the Installed Mail Suite 4

5 Definitions and Terminology **5**

6 Configuring Guardian Digital Mail Suite **6**

6.1 General Configuration 7

6.1.1 Server Configuration 8

6.1.2 Secure User Manager 16

6.1.3 TLS Server Setup 19

6.1.4 TLS Client Setup 24
6.1.5 WebShare Manager 26
6.1.6 Secure List Port 27
6.2 Maintenance and Monitoring 28
6.2.1 Graphs and Reports 28
6.2.2 Queue Maintenance 31
6.2.3 SMS Control Panel 34
6.3 Aliases, Domains, and Routing 35
6.3.1 Mail Aliases 35
6.3.2 Virtual Domains 38
6.4 LDAP Configuration 40
6.4.1 LDAP Configuration 41
6.4.2 LDAP Aliases 42
6.4.3 LDAP Virtual Domains 43

7 Content Policy and Enforcement (CAPE) Center 43
7.1 Mail Filters 44
7.1.1 General Filter Settings 44
7.1.2 Header Filters 50
7.1.3 Body Filters 54
7.1.4 Spam Configuration 55
7.1.5 Virus Configuration 74
7.1.6 Spam/Virus Scanner Exemptions 77
7.2 SMTP Access Controls 78
7.2.1 Recipient Address Access Controls 78
7.2.2 Sender Address Access Controls 79
7.2.3 SMTP Client Access Controls 80
7.3 Recipient Policy 82

7.3.1 Creating a New Protected Domain 83
7.3.2 Adding Protected Addresses 83
7.4 Spam/Virus Quarantine 83
7.4.1 Search Criteria 84
7.4.2 Viewing Messages 85
7.4.3 Deleting Messages from Quarantine. 85
7.5 Disclaimer Footer 85

8 Configuring the LDAP Database **87**
8.1 LDAP Configuration 87

9 Configuring Webmail **89**

10 Public Address Books **91**
10.1 Create a New Address Book 91
10.2 Create a New Address Book Entry 93

11 Secure User Manager **95**
11.1 Downloading User E-Mail Certificates 95
11.2 Manage Forwarding Address 95
11.2.1 General Settings 96
11.3 Managing the Vacation Message 96
11.3.1 General Settings 97
11.3.2 Vacation Message 98
11.4 Mail Filter Preferences 98
11.4.1 Point Thresholds 99
11.4.2 Subject Tagging 100
11.4.3 Spam Whitelist 100
11.4.4 Spam Blacklist 101
11.5 Spam/Virus Quarantine 101
11.6 Spam Learning Center 102
11.6.1 Exporting PST Files From Outlook 103

12 Address Books and E-Mail Client Configuration **107**

12.1 Outlook Express 6 107

12.2 Outlook XP 111

12.3 Netscape Messenger 7 115

13 Configuring the E-Mail Client for TLS **118**

13.1 Outlook Express 6 118

13.1.1 Creating a New E-Mail Account 118

13.1.2 Configuring E-Mail Accounts for TLS 124

13.2 Outlook XP 127

13.2.1 Creating a new TLS Enabled Account 128

13.2.2 Enabling TLS on an Existing Account 134

13.3 Netscape Messenger 7 138

13.3.1 Creating a New E-Mail Account 138

13.3.2 Import the TLS Certificate 144

14 Configuring the E-Mail Client for SPOP and SIMAP **149**

14.1 Microsoft Outlook Express 149

14.2 Microsoft Outlook XP 149

14.3 Netscape Messenger 7 149

A What is CIDR Notation **150**

1 Introduction

Welcome to the Guardian Digital Secure Mail Suite!

Built on the foundation of EnGarde v1.5, *Guardian Digital Secure Mail Suite* provides the ability to create a complete email system for an entire organization. Designed to meet the needs of small businesses, enterprise level companies, ISPs and ASPs looking to secure and manage corporate email operations, *Secure Mail Suite* is capable of managing all email functions within an organization.

Secure Mail Suite offers simplified administration capabilities to build a complete enterprise mail environment, and engineered to scale to thousands of users and domains. Through its use of advanced access control and authentication mechanisms, comprehensive auditing and reporting features, anti-spam and anti-virus protection, as well as encrypted communications facilities, *Secure Mail Suit*e delivers protection from constantly evolving online threats for both internal and external mail systems.

This manual will outline exactly how to install and configure the *Secure Mail Suite* for your organization, and how to ensure it always operates reliably and securely.

2 Contacting Guardian Digital

Guardian Digital welcomes your input and feedback. You may direct all questions, commands, or requests concerning the software you purchased, your registration status, or similar issues to the Guardian Digital Customer Service department at the following address:

Guardian Digital Customer Service
165 Chestnut Street
Allendale, New Jersey 07401
United States

Phone:	+1-201-934-9230
E-Mail:	customer.service@guardiandigital.com
World Wide Web:	http://www.guardiandigital.com
Online Store:	http://store.guardiandigital.com

The department's hours of operation are 9:00 AM to 5:00 PM Eastern Time, Monday through Friday.

3 Guardian Digital Master Support

Guardian Digital provides comprehensive support for your enterprise. Guardian Digital can help bridge the gap between the fast-paced nature of the Internet, security, and the latest open source technologies available in EnGarde. Guardian Digital can provide you with the information necessary to develop unique customizations of EnGarde products to achieve the fastest time to market with the most cost-effective solutions.

Guardian Digital encourages you to visit us on the Web for the answers to many commonly asked questions and system documentation. Contact Guardian Digital Master Support between the hours of 9:00 AM and 6:00 PM Eastern time.

To provide the answers you need quickly and efficiently, the Guardian Digital Master Support staff needs some information about your computer and software. Please include this information in your correspondence:

- Program name and version number
- Product registration number
- Any additional hardware or peripherals connected to your computer
- How to reproduce your problem: when it occurs, whether you can reproduce it regularly, and under what conditions
- Information needed to contact you by voice, fax, or e-mail
- Steps you have taken thus far to try to resolve the problem
- Any additional software installed

Please contact us using one of the following methods:

Phone:	+1-201-934-9230
E-Mail:	support@guardiandigital.com
World Wide Web:	http://www.guardiandigital.com

To avoid delay in processing your request, be sure to include your registration number in the subject of the e-mail.

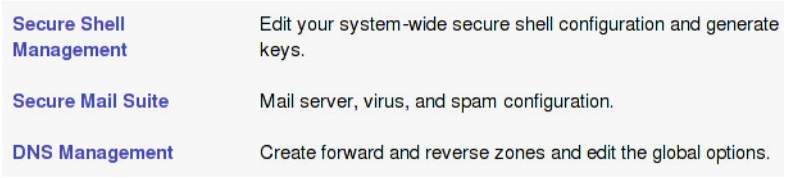
4 Installing Guardian Digital Secure Mail Suite

Guardian Digital Secure Mail Suite is installed via Guardian Digital Secure Network (GDSN). To install the *Secure Mail Suite* insert the CD-ROM disk that was included with the *Guardian Digital Secure Mail Suite* purchase into the CD-ROM drive of the EnGarde server you will be installing the *Secure Mail Suite* on.

Selecting *Install from Local Media* in the GDSN will perform the installation. Instructions on how to use the GDSN can be found in *Section 5* on page *173* of EnGarde Secure Professional User Manual. Additionally the *Install from Local Media* portion can be located on page *175* under *Section 5.1.2 Install from Local Media*.

4.1 Accessing the Installed Mail Suite

Once the GDSN finishes installing all of the *Secure Mail Suite* packages, the *Secure Mail Suite* portion will be accessible from the WebTool located in place of the original *Mail Configuration* option in the *System Management*, now labeled as *Secure Mail Suite*.


Secure Shell Management
Edit your system-wide secure shell configuration and generate keys.
Secure Mail Suite
Mail server, virus, and spam configuration.
DNS Management
Create forward and reverse zones and edit the global options.

5 Definitions and Terminology

Before we begin it is important that you, the reader, are familiar with some of the terminology used throughout this documentation and the WebTool. Please read and understand the terms below before proceeding.

ACL Access Control List. List of users who may access a feature.

Bayes Filter A spam filtering method that classifies mail using information it has learned from previous mail.

Body Part of email that contains the mail content excluding the Header.

Certification Authority An entity that issues digital (X.509) certificates and vouches for the data contained in such certificates. A CA may be thought of as a trusted third party who *signs* certificates, making them valid.

Corpus Large collection of spam and non-spam mail.

Domain A domain name is a name given to a group of machines. A domain name identifes one or more IP addresses. In an email address, the part to the right of '@' is the domain name.

Envelope The sender and recipient addresses in the SMTP transaction are called the *Message Envelope*. Note that these addresses do not to have to be the same as the addresses in the message headers.

Ham Legitimate mail

Header Information at the beginning of an email. Message headers contain the addresses of sender and recipients, the subject of the message and the date and time the message was received.

Host Name of the machine that receive mail

Host Certificate An X.509 certificate for a machine.

Internet Message Access Protocol A protocol for retrieving e-mail from a mail server. Commonly referred to as IMAP, a connection remains open to the server while mail is being read. Mail is stored remotely on the server unless specified by the e-mail client to download and store the mail locally.

LDAP Lightweight Directory Access Protocol. It is a protocol for acessing information directories such as addresses, phone numbers, etc

Mail Relay A server that routes an email to the correct destination. Mail relays are used to forward all mail for the local domain to the mail store.

Mail Store The server that receives and stores mail for a domain. Mail Store is the final destination for a particular domain.

MIME Multipurpose Internet Mail Extensions. It refers to an official Internet standard that specifies how messages must be formatted so that they can be exchanged between different email systems.

Post Office Protocol A protocol for retrieving e-mail. Also referred to as POP3 (version 3), it downloads all new e-mail messages from the server and stores them locally on a users machine.

PST Format of MS Outlook mail archives.

Remote Certificate An X.509 certificate issued on a machine other then the local one. Remote Certificates are not signed by the local Certification Authority and are usually used to identify a machine on the other end.

Shared Key A string (much like a password or a pass-phrase) that is shared between the TLS mail server and client used for authentication.

Simple Mail Transfer Protocol A protocol for sending e-mail messages between servers. Also commonly referred to as SMTP.

Spam Illegitimate bulk mail

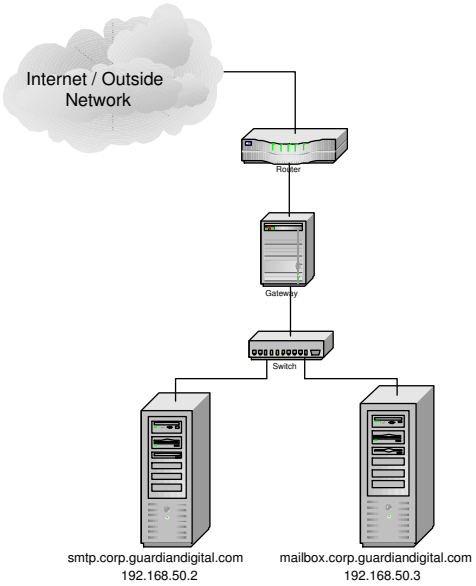
User Certificate An X.509 certificate for a person. A User Certificate may be associated with a local user on the machine.

Virtual Domain A domain that exists as a software entity on the server, which doesn't need a dedicated hardware location. A server can receive mail for a virtual domain.

X.509 Certificate The standard format for digital certificates.

6 Configuring Guardian Digital Mail Suite

For this manual all examples will apply a real-life setup. The setup being used will have a main SMTP server which will act as a mail relay to a mailbox/spool server that stores the mail. The following diagram outlines this configuration:



We will be using the `192.168.50.0/24` network (*corp.guardiandigital.com*) for our example. The two mail servers will be

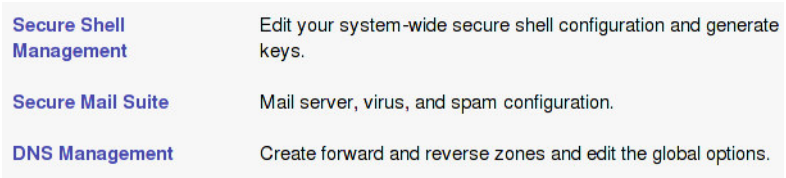
`192.168.50.2` (*smtp.corp.guardiandigital.com*)
`192.168.50.3` (*mailbox.corp.guardiandigital.com*)

Generally these two mail servers will be the only mail servers located on the network they are on and will be protected by a firewall. Additionally, depending on the network configuration, DNS service may be required. However, both the configuration of a firewall and DNS is beyond the scope of this document.

NOTE: The network `192.168.50.0/24` is being displayed in CIDR notation. For an explanation of this method refer to *Appendix A* on page *150*.

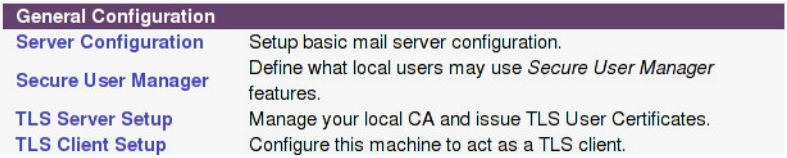
6.1 General Configuration

Secure Mail Suite can be found in the *Service Configuration* section in the *System Management* portion of the WebTool.



Secure Shell Management	Edit your system-wide secure shell configuration and generate keys.
Secure Mail Suite	Mail server, virus, and spam configuration.
DNS Management	Create forward and reverse zones and edit the global options.

Once the *Secure Mail Suite* option is selected from the *System Management* menu the *Guardian Digital Secure Mail Suite* menu will appear with a number of options.



General Configuration	
Server Configuration	Setup basic mail server configuration.
Secure User Manager	Define what local users may use *Secure User Manager* features.
TLS Server Setup	Manage your local CA and issue TLS User Certificates.
TLS Client Setup	Configure this machine to act as a TLS client.

The *General Configuration* portion is the first step to be completed. This section is broken down into the *Server Configuration*, *Secure User manager, TLS Server Setup, TLS Client Setup* categories. Each of these categories is outlined in the following sections.

6.1.1 Server Configuration

The *Server Configuration* section is broken down into several smaller pieces. Here basic settings for the mail server such as *domain name, relay host, queue settings, client restrictions*, and *local networks* can be defined.

General Configuration

The *General Configuration* contains the settings for the basic functionality of the mail server.

Machine Hostname This is where the mail server's hostname is entered.

In the example above this would be the configuration for the *mailbox.corp.guardiandigital.com* machine.

Relay Host If the machine needs to pass mail to another mail server to get out to the Internet, the hostname of the mail server should be defined as the *Relay Host*. If a *Relay Host* is defined, mail to all domains not defined as a mail route or virtual domain, will be forwarded to the machine defined as *Relay Host.*

In the above example, mail is being relayed out to the Internet through the relay server *smtp.corp.guardiandigital.com*. so *smtp.corp.guardiandigital.-com* was used here.

Backup Relay Host If there is a secondary mail server that will be receiving mail from this server, the address of the server would be entered here.

This server will automatically be used in circumstances where the primary relay host is inaccessible for sending outbound mail.

In our example there is only one server to relay mail to, *smtp.corp.guardi-andigital.com*, so this field remains blank.

Always BCC: Address If an email address is entered in here, a copy of each mail received by this server will be sent to that address. This field is optional. If mail to the BCC address bounces, the bounced message will be sent to the sender.

POP Before SMTP A user outside the network with POP access to the server can receive their e-mail, however they can not send e-mail due to security

restrictions. What this option does is allow POP to verify the user. Once the user uses POP to check their e-mail they will then be allowed to send mail through the server.

Set this option to *Enabled* if outside POP users need to send e-mail from the server. If users are using Microsoft Outlook this feature needs to be enabled.

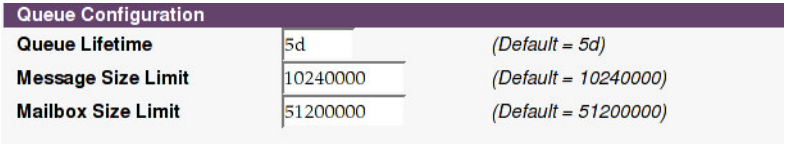
NOTE: It will also be necessary to configure the user's mail client to use this feature.

Grace Period If *POP Before SMTP* is enabled this determines the amount of time, in minutes, that a user is valid, before being required to re-authenticate themselves by checking their e-mail via POP.

Configuring this for around 10 to 15 minutes is reasonable.

Queue Configuration

The *Queue Configurations* allows limitations such as *Queue Lifetime*, *Message Size Limits* and *Mailbox Size Limits* to be set.



Queue Lifetime When mail is sent or received it first goes in to a queue. When the destination mail server responds and accepts the recipient message it will be removed from the queue and delivered to the user. However if the mail server recipient is not responding or is unreachable, it will wait in the queue until it can be delivered later.

This options determines how long the e-mail message will wait in the queue before being deleted. The default value is 5 days. While in the queue the mail server will keep trying to send it by default every 1000 seconds (16 minutes 40 seconds).

Message Size Limits This determines the maximum size a message is allowed to be. This includes the body of the message and any attachments.

This size limit is in bytes. So in the example above it's 10240000 bytes, 10240KB or 10MB.

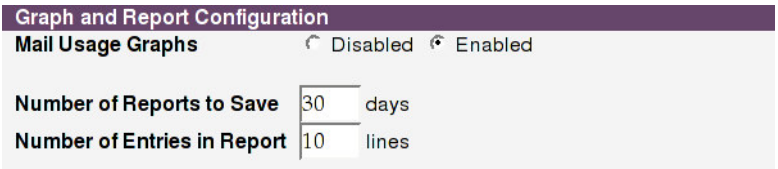
Mailbox Size Limits Each user with an e-mail account has their mail stored on some mail server. This option determines the maximum size a users mailbox is allowed to reach. If the user exceeds this size e-mail will be rejected when the server receives it.

As with the *Message Size Limits*, this number is also in bytes.

Graph & Report Configuration

Secure Mail Suite creates graphs and reports. The graphs display sent, received, bounced and rejected mail over time. The reports breakdown the e-mail traffic over the past 24 hour period with more detailed statistics than the graphs can provide.

In the *Report Configuration* section a few report options can be configured.



Mail Usage Graphs You can enable or disable mail usage graphs here.

Number of Reports to Save Reports are created on a daily basis and stored on the server for reference. This option determines how long a report will stay on the server. Once the specified interval is reached the report will be removed from the server and will no longer accessible.

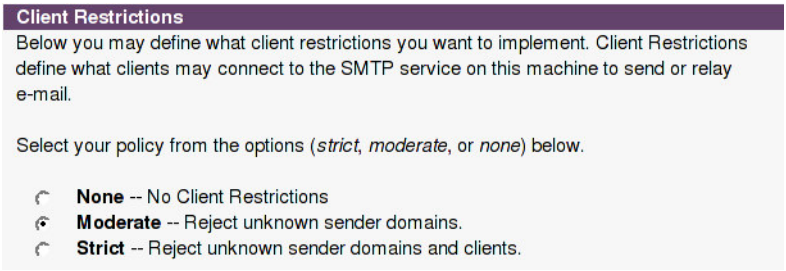
Number of Entries in Report A portion of the reports, generated by the mail server, contain listings of different statistics sorted by count. These lists can grow quite large on servers with a good deal of traffic. The list will be limited to the number of entries specified here.

Generally a value of *10* is reasonable amount.

Client Restrictions

This section allows high-level, general policies of *Client Restrictions* to be configured. The *Client Restrictions* define a *first cut* at what clients may connect to the mail server on this machine. Fine tuning of these restrictions will be discussed later in section *6.3.1*. Depending on the setting here the mail server will determine if the user's e-mail can be sent, relayed or rejected.

These helps prevent unknown machines and possibly spam from being sent through the server.


Client Restrictions
Below you may define what client restrictions you want to implement. Client Restrictions define what clients may connect to the SMTP service on this machine to send or relay e-mail.
Select your policy from the options (strict, moderate, or none) below.
None -- No Client Restrictions
Moderate -- Reject unknown sender domains.
Strict -- Reject unknown sender domains and clients.

None Selecting *None* removes all client restrictions. All connecting mail servers will be able to send mail to this server if the destination is valid for this server. This option should be avoided.

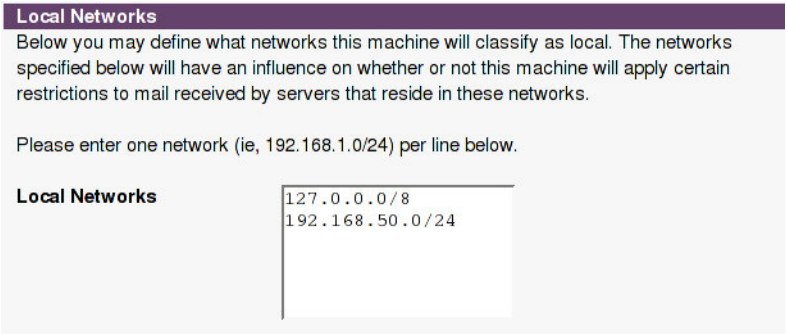
Moderate Selecting *Moderate* rejects mail if either the sender domain or the recipient domain is not a FQDN (Fully Qualified Domain Name) or cannot be resolved by DNS. It will also reject mail if the sender hostname is in invalid format. This is the recommended setting.

Strict Selecting *Strict* sets the mail server to reject any incoming mail where the sender's hostname can't be resolved by DNS, in additions to all other restrictions at the *moderate* level. This option may cause some legitimate mail to be rejected.

Local Networks

The *Local Networks* section defines what machines are considered *trusted* based on their network address. These machines will be exempt from all the restrictions

set in *Client Restrictions*. All machines in the local networks will be able to relay mail through this server.


Local Networks
Below you may define what networks this machine will classify as local. The networks specified below will have an influence on whether or not this machine will apply certain restrictions to mail received by servers that reside in these networks.
Please enter one network (ie, 192.168.1.0/24) per line below.
Local Networks
127.0.0.0/8
192.168.50.0/24

In the entry box the default `127.0.0.0/8` will be in place. On a new line enter the CIDR notation of each additional network.

NOTE: For an explanation of CIDR notation refer to *Appendix A* on page *150*.

In the example network setup used in this documentation the *smtp.corp.guardiandigital.com* machine will be relaying mail for the *corp.guardiandigital.com* to *mailbox.corp.guardiandigital.com*. *corp.guardiandigital.com* is the local network `192.168.50.0/24`. So, as in the example above, `192.168.50.0/24` is required.

Domain Spoof Protection

This section allows you to define *external* and *internal* domains to be protected from spoofed *From:* headers intended to impersonate your mail domains. In other words, no incoming messages with a *From: user@domains.com* will be accepted where *domains.com* matches the listed domains below.

Please note that you MUST have your local networks listed correctly in *Local Networks* above in order for this to work properly.

It is recommended that you enable this functionality and use the *Create additional entry for all sub-domains* feature to cover all of your sub-domains as well.

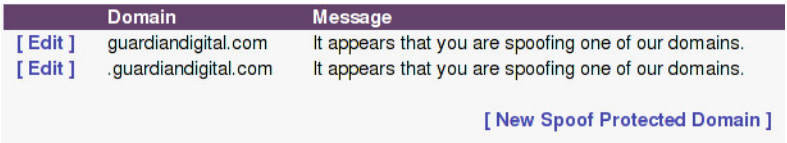
A new domain can be added by selecting *New Spoof Protected Domain*.

A new menu will appear with the options to create this new *Spoof Protected Domain*.

Domain Enter the domain that is to be spoof protected into the *Domain* entry box.

Message When an incoming e-mail is received from a spoofed domain the message in the *Message* entry box will be attached to the rejected e-mail.

Create additional entry for all sub-domains Check this box to protect all sub-domains of the top level domain specified.

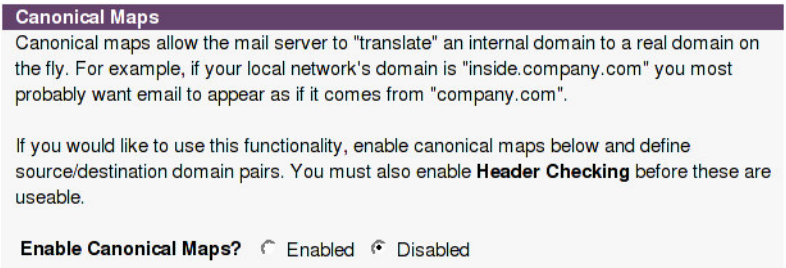

Domain
Message
[Edit] guardiandigital.com It appears that you are spoofing one of our domains.
[Edit] .guardiandigital.com It appears that you are spoofing one of our domains.
[New Spoof Protected Domain]

Once changes have been made click the *Create Domain* button to continue.

The new domain will be listed on the menu. To edit or delete a domain select the *Edit* link found to the left of the domain that is to be edited or deleted. A new menu will appear similar to the *Spoof Protected Domain Creation* menu with the option to save changes or delete the domain. In this example, the a mail with a from address *user@guardiandigital.com* will be rejected by this mail server. Also, the entry *.guardiandigital.com* stands for all the sub-domains under *guardiandigital.com*, like *corp.guardiandigital.com*.

Canonical Maps

Canonical Maps allow the server to translate a non-publicly addressable *internal* domain name into an addressable public domain name.


Canonical Maps
Canonical maps allow the mail server to "translate" an internal domain to a real domain on the fly. For example, if your local network's domain is "inside.company.com" you most probably want email to appear as if it comes from "company.com".
If you would like to use this functionality, enable canonical maps below and define source/destination domain pairs. You must also enable Header Checking before these are useable.
Enable Canonical Maps? Enabled Disabled

Using the example in this document, the server is located in the *corp.guardiandigital.com* domain. If we have a user *nick* the e-mail address would be *nick@corp.guardiandigital.com*. However in our example *corp.guardiandigital.com* is in the non-policy addressing IP space of *192.168.50.0/24*. So on *smtp.guardiandigital.com* we define a canonical mapping for this domain to translate to the real domain of *guardiandigital.com* (209.11.107.14). Doing this makes the translation of *nick@corp.guardiandigital.com* to *nick@guardiandigital.com* publicly addressable.

Once *Canonical Maps* are enabled the source domain and destination domain needs to be defined for every non-publicly addressable *internal* domain hosted by *mailbox.corp.guardiandigital.com* in which users will be sending mail to the Internet for the above example to be complete.

You need to enable *Header Filters* before using the canonical maps. This can be done in the *Header Filters* page accessible from the *Mail Filters* section in the *Content And Policy Enforcement (CAPE)* center of the *Secure Mail Suite*. You don't need to create any entries in the *Header Filters* section.

Creating a New Canonical Map

To create a new canonical map click on the *New Canonical Map* button. A new menu will appear.

Source Domain This is the domain that was described above as the *internal* domain. The domain that the map will be coming from.

In our example *corp.guardiandigital.com* was entered here so that e-mail will be sent and received from *user@corp.guardiandigital.com* but the external address will appear as *user@destination_domain*, *guardiandigital.com* in this example.

Destination Domain This is the domain that will be the one visible.

In the example used above *guardiandigital.com* was entered here. This allows e-mail address to be seen as *user@guardiandigital.com*.

Once the fields have been filled in and the new canonical map is created, it will be displayed in the *Canonical Maps* section. Clicking the *Edit* link to the left of the map will allow it to be edited.

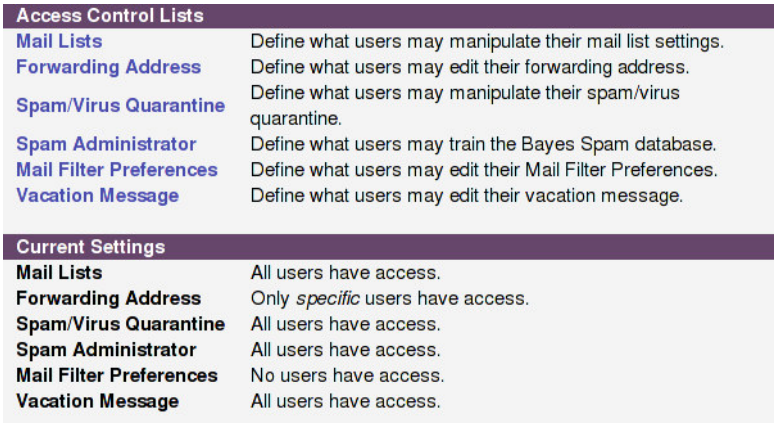
At this point the general configuration is completed. Click the *Save Configuration* button to save all the changes made.

NOTE: This scenario applies well where there is a mail server that relays the mail to a mailbox server where there is only one internal domain.

When multiple internal domains are canonically mapped extra virtual and transport mapping may be required.

6.1.2 Secure User Manager

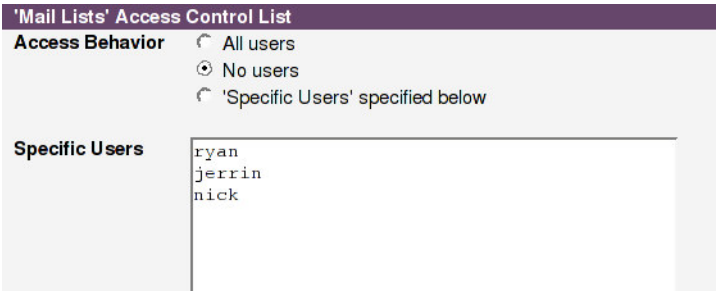
This section defines what local users will be allowed to access specific *Secure User Manager* features. Most of the features are accessible by all local users by default. On this page, you can control user access in the *mail lists, forwarding address*, *virus/spam quarantine, spam administrator, mail filter preferences* and *vacation message sections.* Here you define what users may access these features available in the *Secure User Manager*.


Access Control Lists
Mail Lists
Define what users may manipulate their mail list settings.
Forwarding Address
Define what users may edit their forwarding address.
Spam/Virus Quarantine
Define what users may manipulate their spam/virus quarantine.
Spam Administrator
Define what users may train the Bayes Spam database.
Mail Filter Preferences
Define what users may edit their Mail Filter Preferences.
Vacation Message
Define what users may edit their vacation message.
Current Settings
Mail Lists
All users have access.
Forwarding Address
Only specific users have access.
Spam/Virus Quarantine
All users have access.
Spam Administrator
All users have access.
Mail Filter Preferences
No users have access.
Vacation Message
All users have access.

Mail Lists

This section defines what local users will be allowed to manipulate their mail list settings. If allowed, a user will able to see mailing lists hosted on this machine, subscribe to a mailing list and manipulate his mail list settings.

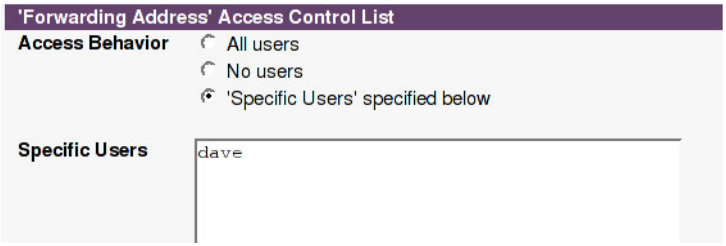
Note Only existing local users can use this feature. This privilege is not necessary for users to subscribe/unsubscribe.



Access Behavior If *All users* is selected, all local users will be able to manipulate their mail list settings. If *No users* is selected, no local user will be able allowed. You can specifically allow certain users by selecting the *Specific Users* option and adding the user names on the *Specific Users* box below. Enter one user per line. In this case, only those users listed here will be allowed to edit their mailing list settings.

Forwarding Address

This section defines what users will be allowed to edit their forwarding addresses. If allowed, a user can forward all mail delivered to him to another email address. To access this section, click on the *Forwarding Address* link on *Access Control Lists* section.



Access Behavior If *All users* is selected, all local users will be able to edit their forwarding addresses. If *No users* is selected, no local user will be able to edit their forwarding addresses. You can specifically allow certain users by selecting the *Specific Users* option and adding the user names on the *Specific Users* box below. Enter one user per line. In this case, only those users listed here will be allowed to edit their forwarding addresses.

Spam/Virus Quarantine

This section defines what users are allowed to see their quarantine messages. Allowed users can view the quarantined messages for which they are either sender or recipient. They can forward or delete the quarantined mail. To access this section, click *Spam/Virus Quarantine*. Configuring this section is similar to the *Mail Lists* and *Forwarding Address* sections above.

Spam Administrator

This section defines what users will be allowed to train the Bayes Spam database. If allowed, a user can upload his spam/ham files in PST format using the *Secure User Manager*. The uploaded ham/spam files will be learned by the Bayes subsystem of the spam filter, which can greatly improve its efficiency. To access this section, click on the *Spam Administrator* link on *Access Control Lists* section.

Access Behavior This section defines what users may train the Bayes Spam database. Like other *Access Control Lists* above, we can either allow all users, deny all users or allow only specific users listed on the *Specific Users* box.

Be careful to only add trusted users to this ACL. Adding untrusted users is dangerous because they can maliciously upload false ham/spam and poison your Bayes database.

Mail Filter Preferences

This section defines what users will be allowed to edit their mail filter settings. Configuring this section is similar to the sections described above.

Vacation Message

This section defines what users will be allowed to edit a vacation message. The vacation message is an auto-reply to be sent to email senders if the local recipient is unavailable. If allowed, a user can set up a vacation message for himself. To access this section, click on the *Vacation Message* link on the *Access Control Lists* section. Configuring this section is similar to the *Forwarding Address* and *Spam Administrator* sections above.

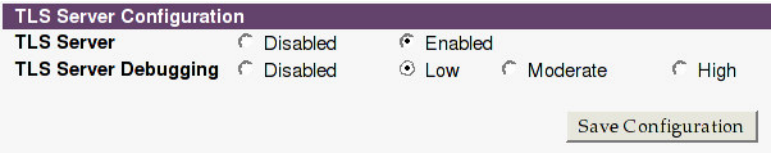
6.1.3 TLS Server Setup

The *TLS Server Configuration* allows TLS support in the *Secure Mail Suite* to be enabled along with all the necessary certificates.

A TLS enabled mail server allows user authentication for relay access to the server via the certificate key method. This is used primarily for roaming users but can also be used to verify other servers on the Internet that would be allowed to relay through the mail server.

TLS Server Configuration

In the *TLS Server Configuration* section there is the ability to enable/disable the TLS capabilities in the mail server. Additionally there are debugging options here.



TLS Server The *TLS Server* has the option to be *Enabled* or *Disabled*. The *TLS Server* can not be enabled until all the necessary certificates have been created. For information concerning creation of these certificates, follow this section.

TLS Server Debugging The *TLS Server Debugging* allows different levels of debugging verbosity to be logged. If there are problems getting TLS to work in the setup it's being used in, debugging can be enabled. More verbose information will be written to the mail log. You can view the mail log from *Secure Mail Suite Control Panel* (section 6.2.3 on page 34). This way when attempting to debug TLS the logs can be watched in a real-time manner.

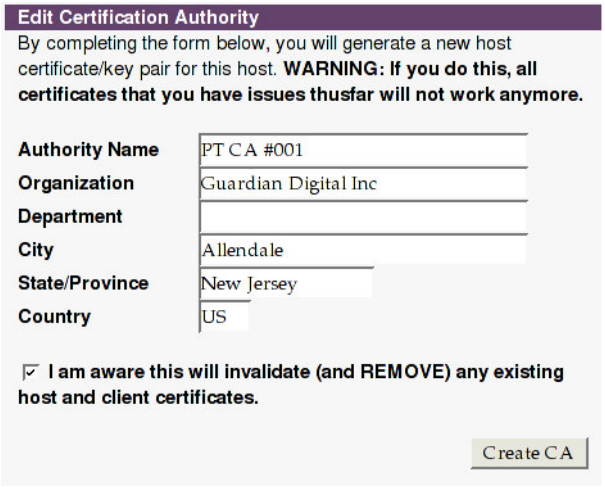
Certificate Authority

A *Certification Authority* (CA) is an entity which vouches for the accuracy of data on a digital certificate by signing it.

Think of a CA as a notary public. You need to send an important letter to somebody so you take it to a notary public who stamps it. When the recipient receives your letter they will trust it because of the verification this neutral third-party provides.

Much like the scenario given above, the CA you create in the WebTool will sign digital certificates which are issued to other hosts and users.

To set up your CA click the *Edit* link under *Certification Authority*. An example setup:


Edit Certification Authority
By completing the form below, you will generate a new host certificate/key pair for this host. WARNING: If you do this, all certificates that you have issues thusfar will not work anymore.
Authority Name
PT CA #001
Organization
Guardian Digital Inc
Department
City
Allendale
State/Province
New Jersey
Country
US
I am aware this will invalidate (and REMOVE) any existing host and client certificates.
Create CA

Once all the fields have been completed click *Create Certificate* to create this new CA. All fields are required except for the *Department* field.

Once a CA is created it should only be deleted when you want to *start over* again. Re-creating a CA will in effect nullify any certificates that have been issued.

Once the CA is created it will be listed below in the *Certificate Authority* section.

Host Certificate

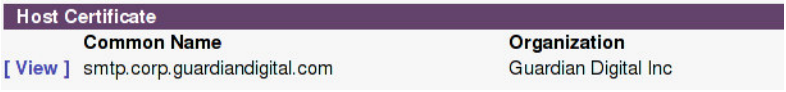
The *Host Certificate* is a X.509 certificate used by the TLS server only and is required.

To create the new *Host Certificate* click the *Edit* link below the *Host Certificate* portion of the menu. This will open up a new window containing the required fields for this new certificate.

Edit Host Certificate
Below you may created/edit/delete a host certificate. Please make sure you enter the fully-qualified domain name of the host (ie, smtp.guardiandigital.com) in the 'Authority Name' field.
Authority Name
smtp.corp.guardiandigital.com
Organization
Guardian Digital Inc
City
Allendale
State/Province
New Jersey
Country
US
I am aware that once a certificate has been created it may not be edited, only removed.
Create Certificate

Once all the fields have been completed click *Create Certificate* to create this new CA.

Once a *Host Certificate* is created it should only be deleted when you want to start over again. Re-creating the *Host Certificate* will replace the prior host certificate.



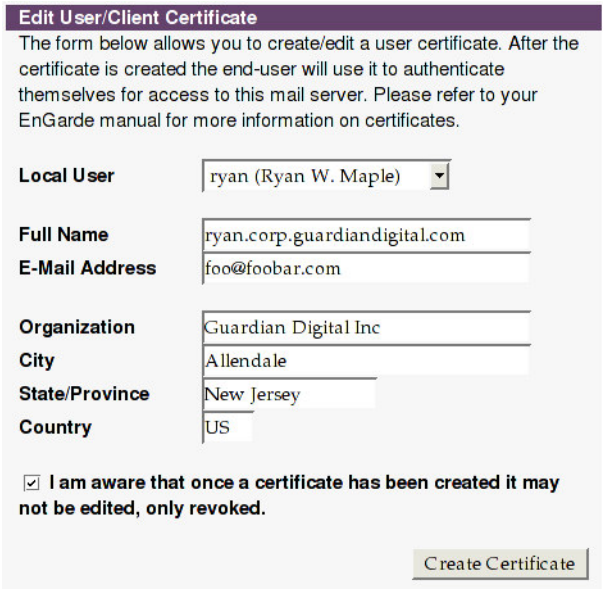
Once the *Host Certificate* is created it will be listed below in the *Certificate Authority* section.

User TLS Client Certificates

A *User Certificate* is an X.509 certificate intended to be issued to another person (for example, an employee who works from home or a TLS client). A TLS client can upload a certificate that has been previously downloaded from the CA/TLS Server, see *Downloading a User Certificate*.

Creating a New User Certificate

To add a new *User Certificate* click the *New User Certificate* link. A new window will appear with the appropriate fields needed to create this certificate.


Edit User/Client Certificate
The form below allows you to create/edit a user certificate. After the certificate is created the end-user will use it to authenticate themselves for access to this mail server. Please refer to your EnGarde manual for more information on certificates.
Local User
ryan (Ryan W. Maple)
Full Name
ryan.corp.guardiandigital.com
E-Mail Address
foo@foobar.com
Organization
Guardian Digital Inc
City
Allendale
State/Province
New Jersey
Country
US
I am aware that once a certificate has been created it may not be edited, only revoked.
Create Certificate

Once all the fields have been completed click the *Create Certificate* button to have this certificate created.

NOTE: The *Full Name* field in this User Certificate is not the user name but is instead the host name of the server this user will be attempting to make a connection from.

If this is a certificate for a TLS client leave the *Local User* field blank and put the client hostname in the *Full Name* field instead.

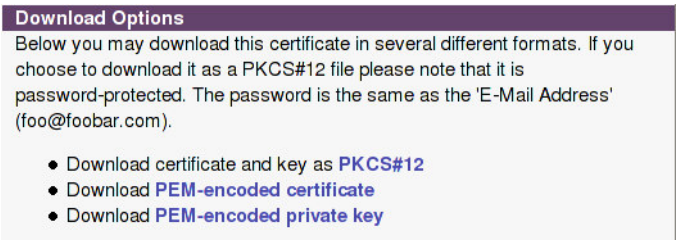
After clicking *Create Certificate* the new certificate will be listed below the *User Certificates* portion of the menu . Please note that if a *Local User* is selected the created certificate will be available for them to download in the *Secure Manager*.

NOTE: Remember the *e-mail address* field is also the password needed to import the certificate later on.

Downloading a User Certificate

To download a *User Certificate* click the *View* link found next to the certificates *Common Name* in the *User Certificates* section. Use the links in the *Download*

Options section to download the certificate and/or private key in the desired format. The PKCS#12 format is the most commonly used format by other machines and browsers for importing.


Download Options
Below you may download this certificate in several different formats. If you choose to download it as a PKCS#12 file please note that it is password-protected. The password is the same as the 'E-Mail Address' (foo@foobar.com).
Download certificate and key as PKCS#12
Download PEM-encoded certificate
Download PEM-encoded private key

Revoking a User Certificate

Certificates are never deleted because deleting the certificate from the local machine does not delete it from the remote machine to which it was issued. Therefore instead of removing certificates from the local machine, they are revoked.

The CA keeps a database of what certificates were issued to whom, when, and whether or not the certificate is valid. Revoking a certificate marks it as *INVALID* in the database.

To revoke a *User Certificate* click the *View* link next to its *Common Name*. The *Edit User Certificate* screen will appear. Check the *I am sure I want to revoke this certificate* check-box.

Finally click *Revoke Certificate* to complete the process. The certificate will remain in the listing but will appear with lines through it, indicating it is no longer valid.

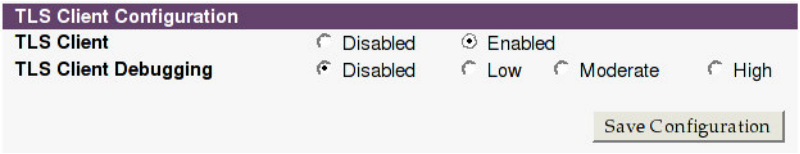
6.1.4 TLS Client Setup

The *TLS Client Configuration* allows TLS support in a client role as opposed to a server role in the *Secure Mail Suite* to be enabled.

A TLS client is specifically designed to configure the mail server to use certificate authentication to TLS enabled mail server. Unlike the *TLS Server Setup* above there is no *User Certificate* portion.

TLS Client Configuration

In the *TLS Client Configuration* section there is the ability to enable/disable the TLS capabilities in the mail server. Additionally there are debugging options here.

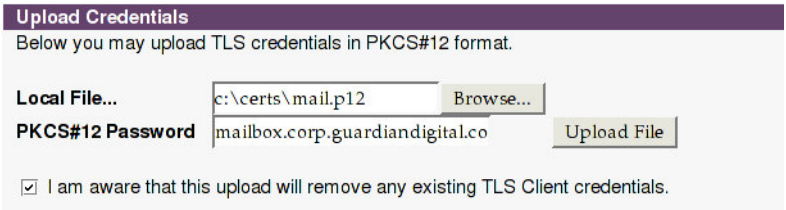


TLS Client The *TLS Client* has the option to be *Enabled* or *Disabled*. The *TLS Client* can not be enabled until the necessary credentials have been uploaded. Perform uploading credentials before setting the configuration with *Enabled* checked.

TLS Client Debugging The *TLS Client Debugging* allows different levels of debugging verbosity to be logged. If there are problems getting TLS to work in the setup it's being used in, debugging can be enabled. More verbose information will be written to the mail log. You can view the mail log from *Secure Mail Suite Control Panel* (section 6.2.3 on page 34). This way when attempting to debug TLS, the logs can be watched in a real-time-like manner.

Upload Credentials

The TLS enabled mail server that this server will be authenticating against first has to create a PKCS#12 certificate for this machine to use TLS for authentication. Now the certificate will be uploaded here. Next, this certificate has to be downloaded to the client machine via the WebTool by the user. This is required if a TLS secured connection is to be initiated between the two mail servers.



Local File Enter the location of the file to be uploaded on the local machine. Choosing the *Browse...* button will bring up a new window that will allow you to browse through the local files on the machine to choose the certificate that was previously downloaded from the TLS server/CA.

PKCS#12 Password Enter the password for the certificate about to be uploaded. This password will be the e-mail address that was entered during the creation of the certificate.

Once both fields are completed, check the *I am aware that this upload will remove any existing TLS Client credentials* check-box and click *Upload File*.

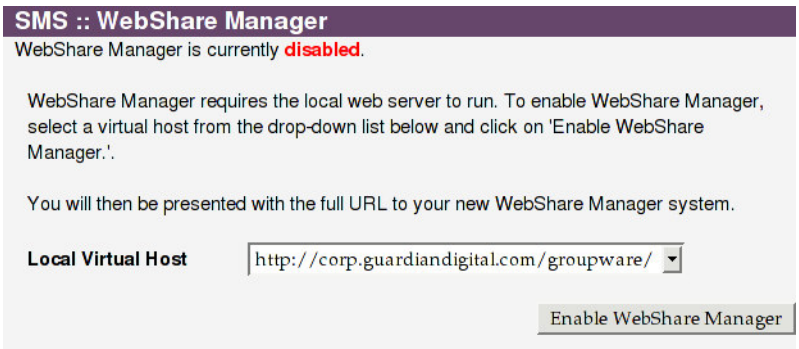
NOTE: This will overwrite any previous certificates stored on the server.

Once the certificate is uploaded the *Common Name* of the CA will appear under the *Certificate Authority* and the *Common Name* of the subject of the certificate (should be the hostname of this machine) will appear under the *Host Certificate* sections. Information pertaining to each certificate can be found by clicking the *View* link found to the left of the respective certificate.

6.1.5 WebShare Manager

Guardian Digital *Secure Mail Suite* includes *WebShare Manager* package. This package includes *user administration, calendaring*, and other features for scheduling.

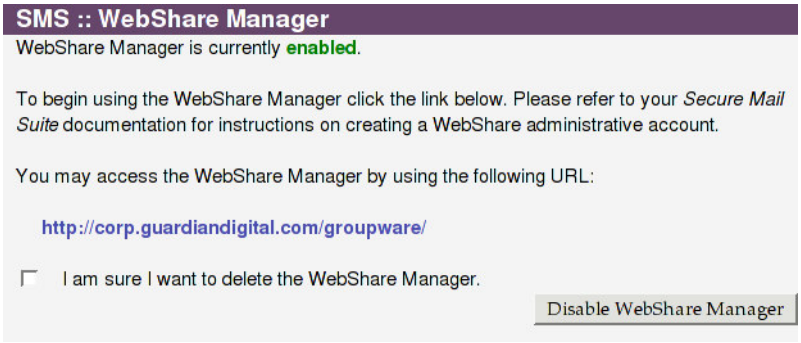
The *WebShare Manager* can be found in the WebTool in the *Guardian Digital Secure Mail Suite* menu under *General Configuration*. Select the *WebShare Manager* link to bring up the menu.


SMS :: WebShare Manager
WebShare Manager is currently disabled.
WebShare Manager requires the local web server to run. To enable WebShare Manager, select a virtual host from the drop-down list below and click on 'Enable WebShare Manager.'.
You will then be presented with the full URL to your new WebShare Manager system.
Local Virtual Host
http://corp.guardiandigital.com/groupware/
Enable WebShare Manager

The *WebShare Manager* menu contains the current state of *WebShare*, this should be disabled if the *Secure Mail Suite* was just installed, along with a list of *Local Virtual Hosts* to enable WebShare on.

NOTE: A virtual host must first be created before WebShare can be enabled. Information regarding virtual hosts can be found in the *EnGarde User Manual* in *section 4.3* on page 56.

From the pull-down menu choose a virtual host and click the *Enable WebShare Manager* button.


SMS :: WebShare Manager
WebShare Manager is currently enabled.
To begin using the WebShare Manager click the link below. Please refer to your Secure Mail Suite documentation for instructions on creating a WebShare administrative account.
You may access the WebShare Manager by using the following URL:
http://corp.guardiandigital.com/groupware/
I am sure I want to delete the WebShare Manager.
Disable WebShare Manager

The menu will refresh with a link to the virtual host with WebShare enabled on it. *WebShare Manager* can be removed from that virtual host by selecting the *I am sure I want to delete the current WebShare Manager* check-box and clicking the *Disable WebShare Manager* button.

NOTE: The default administrative account is *admin* and the password is *admin*.

6.1.6 Secure List Port

Many versions of *Guardian Digital Secure Mail Suite* include mailing list management software called *Secure List Port.* The *Secure List Port* helps you to create and manage mailing lists effortlessly. This section is accessed by clicking *Secure List Port* in *General Configuration*. For information about setting up and maintaining mailing lists, refer to the *Secure List Port User Guide*.

6.2 Maintenance and Monitoring

This section is for monitoring the mail server and doing various maintenance work. This section has three parts: *Graphs and Reports, Queue Maintenance* and *SMS Control Panel.*

6.2.1 Graphs and Reports

The *Graphs and Reports* section contains the most recent mail system reports and mail graphs showing email distribution. Additionally there will be archives of past reports dating back the number of days specified in the *Report Configuration* portion of *General Configuration and Monitoring* section which is documented on page *11* of this guide.

In this screen will be a listing of all the reports in each section and the graphs below that. The reports and graphs are then broken down over time. The graphs and reports are stored for as long as specified in the *Report Configuration* found in the *Server Configuration* section.

Postfix Reports

Postfix Reports					
Report Date	**Size**	**Report Date**	**Size**	**Report Date**	**Size**
May 17th, 2004	501 KB	May 18th, 2004	456 KB	May 19th, 2004	496 KB
May 20th, 2004	560 KB	May 21st, 2004	495 KB	May 22nd, 2004	437 KB

By clicking on a report in the *Postfix Reports* section, a summary of traffic for that day will be displayed.

Postfix Report for May 19th, 2004

Postfix log summaries for May 19

Grand Totals

---

messages

5453 received
8094 delivered
0 forwarded
37 deferred (573 deferrals)
3 bounced
60 rejected

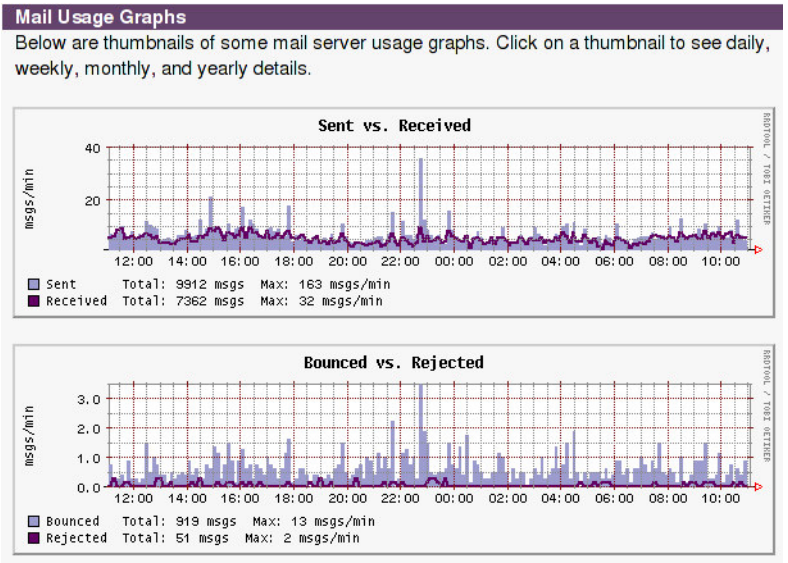
33222k bytes received
46686k bytes delivered
3344 senders
1476 sending hosts/domains
1427 recipients
492 recipient hosts/domains

Per-Hour Traffic Summary

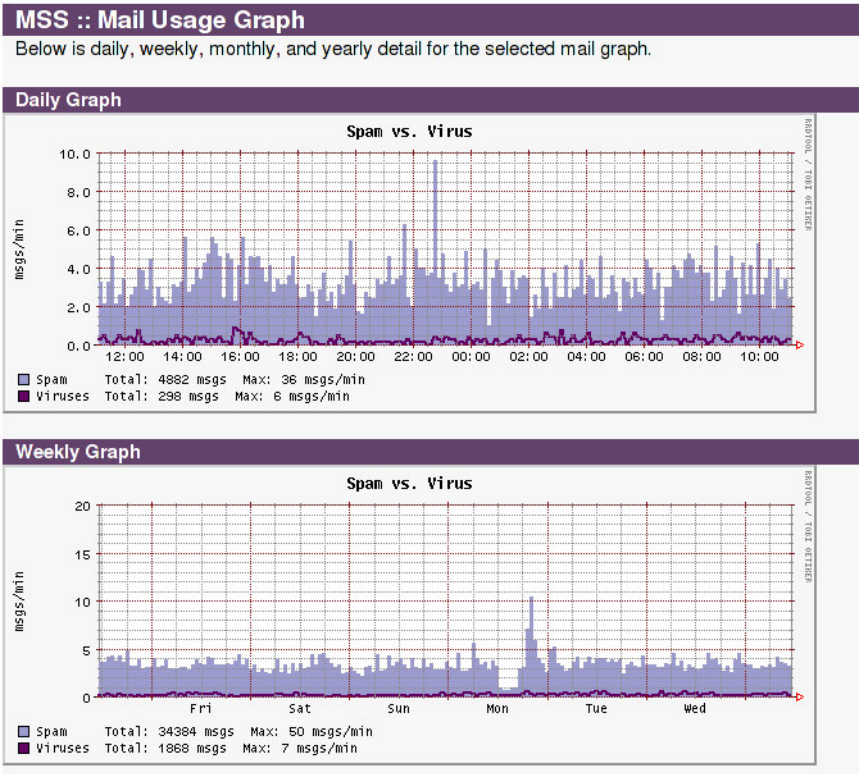
time	received	delivered	deferred	bounced	rejected
0000-0100	184	368	28	1	2
0100-0200	131	274	27	0	0
0200-0300	166	273	26	0	2
0300-0400	206	301	0	0	1
0400-0500	176	232	26	0	4

Postfix Graphs

Mail server usage graphs are shown here in a thumbnail-like fashion, summarizing data.

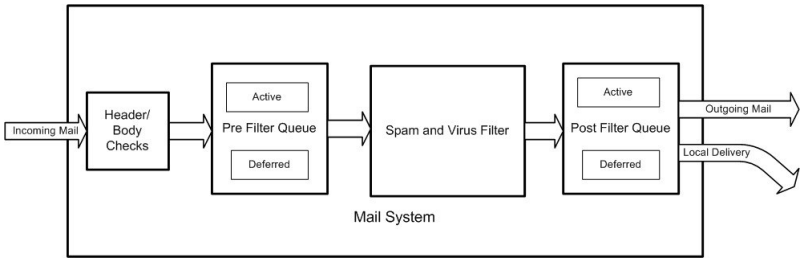

Mail Usage Graphs
Below are thumbnails of some mail server usage graphs. Click on a thumbnail to see daily, weekly, monthly, and yearly details.
Sent vs. Received
msgs/min
40
20
12:00 14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00
Sent Total: 9912 msgs Max: 163 msgs/min
Received Total: 7362 msgs Max: 32 msgs/min
Bounced vs. Rejected
msgs/min
3.0
2.0
1.0
0.0
12:00 14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00
Bounced Total: 919 msgs Max: 13 msgs/min
Rejected Total: 51 msgs Max: 2 msgs/min

By clicking on a graph, a new window will appear with daily, weekly, monthly and yearly detailed graphs.



6.2.2 Queue Maintenance

The *Queue Maintenance* section allows monitoring of messages in the mail queue, flushing and deleting individual messages, and flushing the entire queue. Messages are first placed in the *Pre Filter* queue. The *Pre Filter* queue contains messages waiting to be scanned by the spam/virus filter. When a message is scanned by the filter, it is moved to the *Post Filter* queue. Having a large number of messages in the *Pre Filter* queue could mean that there is a problem in the spam/virus scanner.



Active Messages

The *Active Message* section displays the messages in the queue that are currently being delivered. Once the message is delivered it will be removed from the queue. The messages in the *Pre Filter Active Messages* section contains the messages being received by the mail server.

[Pre Filter] Active Messages

Queue ID	Size	Arrival Time	Sender / Recipient
1F8B1B6343	136593	Thu Jun 17 15:36:51	jerrin@jerrin.inside.guardiandigital.com user@new.guardiandigital.com

To delete or flush a message in the *Active Messages* queue the queue ID can be clicked on. A new window will appear with the contents of the e-mail and the option to delete or flush this e-mail from the queue.

Queue ID 00C11B6393

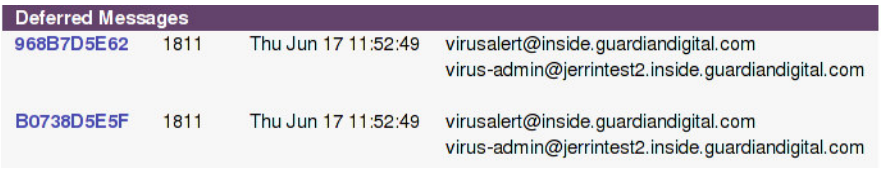
[Click Here] To delete this message from the queue.
[Click Here] To flush this message from the queue.

```
*** ENVELOPE RECORDS /var/spool/postfix/deferred/0/0/00C11B6393 ***
message_size:        136593          368             1
arrival_time: Thu Jun 17 11:36:59 2004
filter:dummy
sender: jerrin@jerrin.inside.guardiandigital.com
named attribute: client_name=jerrin.inside.guardiandigital.com
named attribute: client_address=192.168.1.170
named attribute: message_origin=jerrin.inside.guardiandigital.com[192.168.1.170]
named attribute: helo_name=jerrin.inside.guardiandigital.com
recipient: user@new.guardiandigital.com
```

Deferred Messages

Messages that couldn't be delivered immediately will be listed in the *Deferred Messages* section. By clicking on the message ID, a window containing message details will appear. Additionally in this window will be the option to delete or flush the message from the queue. The *Pre Filter Deferred Messages* list contains the messages that could not be scanned immediately.

Flushing a message consists of forcing the server to attempt to send the e-mail again. If the e-mail fails again, it will be placed back into the queue along with the error message received.



Flushing a message makes the server attempt to send it again. If the problem persists it will end up in the *Deferred Messages* section again.

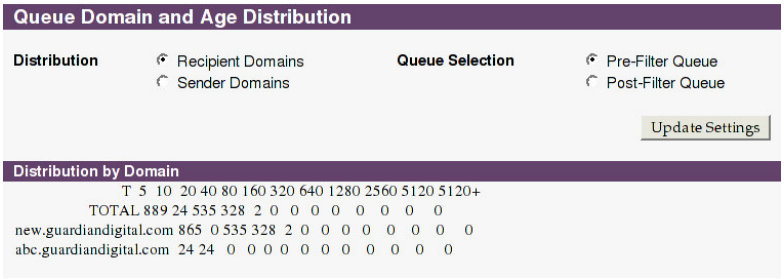
Deleting a message from the queue removes it completely and it will never be delivered.

Flush the Entire Mail System

You can flush all mail in the mail server by clicking on the link displayed on the *Queue Maintenance* page. If the link is clicked, the mail server will try to send all mail in the queue immediately.

Queue Domain and Age Distribution

This section shows the age distribution of mail in the queue for different domains. Click on the link on the *Queue Maintenance* page to view the age distribution. The page shows the number of mail sitting in the queue for different time durations. The first row shows the age of messages in minutes, with the scale doubling. The second row shows the total number of mail with that particular age. All further rows shows the distribution of mail for each domain.

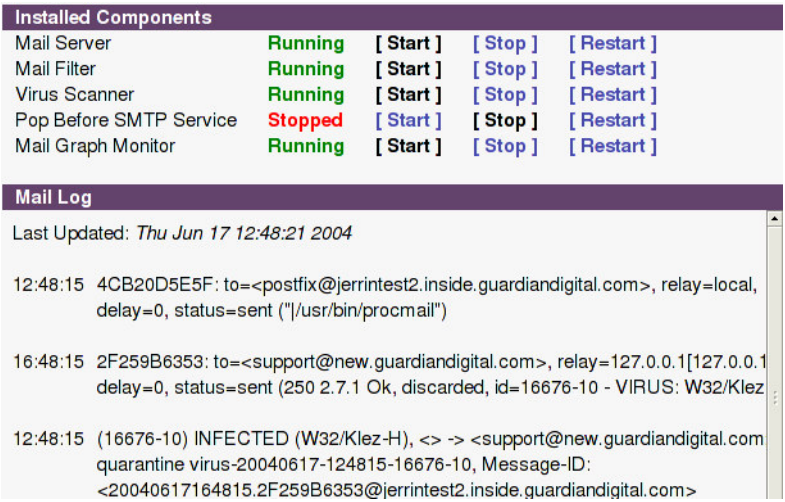


Distribution Select *Recipient Domains* to see the age distribution for messages based on their recipient domains. Likewise, select *Sender Domains* to see the age distribution for messages based on their recipient domains.

Queue Selection You can select the *Pre Filter Queue* or the *Post Filter Queue* here. *Pre Filter Queue* contains messages waiting to be scanned for spam/virus, while the *Post Filter Queue* contains messages that are already scanned and waiting to be relayed.

6.2.3 SMS Control Panel

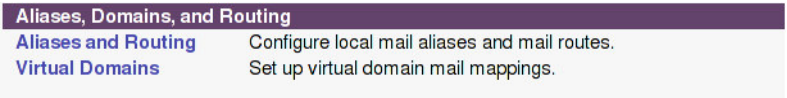
You can start/stop various components of the *Secure Mail Suite* and view the mail log in this section.



Under the *Installed Components* list, different services that belongs to the Secure Mail Suite are shown, along with their current running status. The services may be started, stopped or restarted. The mail log, displayed below shows various messages as they are received, scanned and delivered or relayed in much detail.

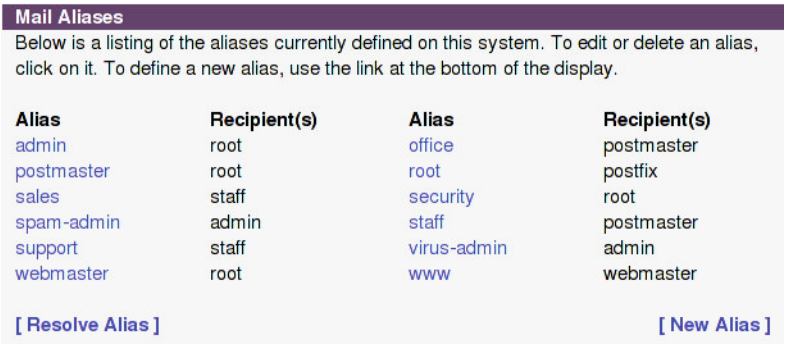
6.3 Aliases, Domains, and Routing

The *Aliases, Domains and Routing* section allows control of user aliases and domain mail routing.


Aliases, Domains, and Routing
Aliases and Routing
Configure local mail aliases and mail routes.
Virtual Domains
Set up virtual domain mail mappings.

6.3.1 Mail Aliases

This section allows you to manage mail aliases. Aliases help you to receive mail for users not existing on the machine. To edit an existing alias click on the name of the alias, not the recipient.



There are two additional option here, *Resolve Alias* and *New Alias*.

NOTE: Only users that are local to the box are allowed to be defined as recipients because aliases are only applied to local delivery.

Resolve Alias

By clicking on the *Resolve Alias* link a new window will appear the option to enter an alias. This does an alias lookup to find the final destination of an alias.

For example, if you have a user *webmaster*, *webmaster* may have an alias to *www*. So that mail to *www@domain.com* will go to webmaster. Additionally you may have another alias, *web* which points to the *www* alias. So if someone sends an e-mail to *web* it will track through the aliases and ultimately be delivered to the *webmaster* account.

Include Resolution Path By selecting this option each individual alias that is part of this resolution path will be displayed.

NOTE: This is only for reference purposes and will not make any changes to the mail server's configuration.

New Alias

A new alias can be created by clicking the *New Alias* link found under *Mail Aliases*.

Alias This is the new alias name being created. E-mail can be sent to this alias and it will automatically be forwarded to the user specified in the *Recipient* field.

Recipient This is the user name that the alias will be forwarded on to. This can be another alias or an actual account on the machine.

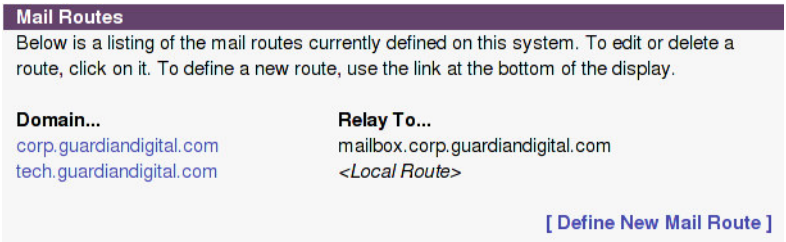
NOTE: If the new alias being created already exists it will overwrite the existing alias.

Mail Routes

The *Mail Routes* section will contain a list of all the mail routes currently on the system. Mail routes are used to forward mail for a domain to the machine serving as mail store for that domain.

Each mail route has a domain name and a destination. If this system is relaying mail it will need a mail route for each domain it is relaying mail for.

In our example setup, the machine *smtp.corp.guardiandigital.com* should relay all mail for the domain *corp.guardiandigital.com* (Eg: mail to *sales@corp.guardiandigital.com*) to the machine *mailbox.corp.guardiandigital.com*. So, a mail route should be created in *smtp.corp.guardiandigital.com* that forwards mail for the domain *corp.guardiandigital.com* to the machine *mailbox.corp.guardiandigital.com*.


Mail Routes
Below is a listing of the mail routes currently defined on this system. To edit or delete a route, click on it. To define a new route, use the link at the bottom of the display.
Domain...
Relay To...
corp.guardiandigital.com
mailbox.corp.guardiandigital.com
tech.guardiandigital.com
<Local Route>
[Define New Mail Route]

To add a new mail route click the *Define New Mail Route* option.

A new window will appear with the fields to create a new rule.

Domain This is the domain whose mail will be relayed on to the final destination. In the example that is being used throughout this documentation, mail is getting relayed for the domain *corp.guardiandigital.com,* through the relay server *smtp.corp.guardiandigital.com* to the mail store *mailbox.corp.guardiandigital.com*. So *corp.guardiandigital.com* is entered in as the domain.

Relay To... Mail can be stored locally or delivered to a remote machine. If ***Local Route*** is selected, mail to the domain will be delivered locally. In this example, mail to *admin@tech.guardiandigital.com* will be delivered to the local user *admin*, since *tech.guardiandigital.com* is defined as a local route.

To relay mail for the domain to a remote machine, select the option *Remote Machine* and enter the hostname of the remote machine below. This is the server that will be the destination for this domain.

As in the example, we want this set to *mailbox.corp.guardiandigital.com,* so mail to the domain *corp.guardiandigital.com* will be sent to the machine *mailbox.corp.guardiandigital.com.*

To edit or delete a route from the *Mail Routes* click on the domain. A new window will appear similar to the window above with the option to delete or update the route.

6.3.2 Virtual Domains

If the mail server is to receive mail for a domain, a *virtual domain* must be configured for each domain for which it is to receive mail. This sections allows configuration of the virtual domains to be handled by the server.

The main screen will display a list of all the virtual domains currently configured on the mail server. To add a new virtual domain click *New Virtual Domain*.

A new window will appear, *Create Virtual Domain*.

Virtual Domain This is the domain for which the server will be receiving mail.

In the example being used in this document we want to receive mail for *corp.guardiandigital.com*. So we would set the virtual domain to that.

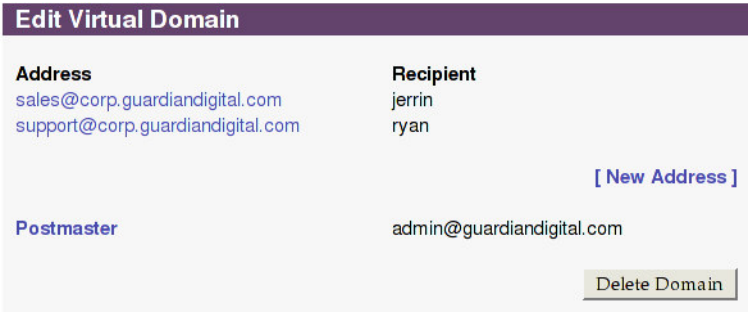
Postmaster The postmaster is an e-mail address of a real user that will act as a default (sometimes called a "catchall") e-mail address. In the event that an e-mail is sent to a user that doesn't exist in the virtual domain, the postmaster of that domain will receive the mail. This is an optional field. If the postmaster is not defined, mail to unknown users will be rejected.

NOTE: In the example being used in this section the relay mail server, *smtp.corp.guardiandigital.com* would not have this virtual domain set on it. It is relaying mail for that domain, not receiving it. (It would have a mail route for this virtual domain instead which would redirect the mail to its final destination).

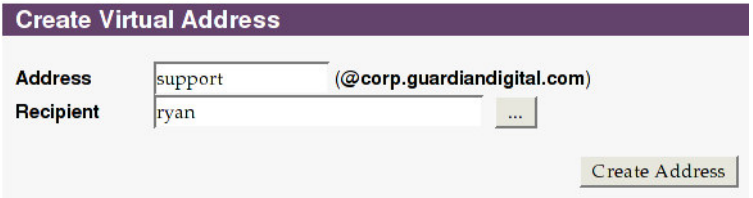
This virtual domain would be configured on the *mail.corp.guardiandigital.com* server instead.

Once all the required fields have been completed click *Create Domain* for this domain to be created.

Once the virtual domain is added, it will be displayed on the list of virtual domains on the main screen. To edit a virtual domain click on the domain. A new window will appear similar to the *Create Virtual Domain* menu. Here the options to delete or update the virtual domain can be found.



To add new addresses to this virtual domain, click *New Address*. Now you can enter an *Address* and a *Recipient*. Click *Create Address* to create this address. The mail server will receive mail for the *Address*, and forward it to the *Recipient*. The recipient can be a local user-name or a full email address. All created virtual domain addresses will be displayed on the *Edit Virtual Domain* window. In this example, the mail server will receive mail for *support@corp.guardiandigital.com* and deliver them to the local user *ryan*.



6.4 LDAP Configuration

Secure Mail Suite can take advantage of the included LDAP server. It can use this server to manage *Aliases* and *Virtual Domains* for your mail servers. This LDAP server can be located on the current server or remotely on another EnGarde machine running *Secure Mail Suite*. Using the latter method provides consistency across all the mail servers.

6.4.1 LDAP Configuration

The basic LDAP configuration allows the configuration of the LDAP server for the postfix mail server. This can be a remote LDAP server found on another EnGarde machine running *Secure Mail Suite* or it can be the local LDAP server.

Note: The LDAP server can be located on a machine not running EnGarde only if the LDAP server's directory structure follows that of *Secure Mail Suite's* LDAP server.

LDAP Server This entry box requires either the IP address or FQDN of the LDAP server. If the LDAP server is located on the current machine a value of *localhost* may be used.

Distinguished Name The *Distinguished Name* is the top level search DN that Postfix will be using. If the LDAP server is on an EnGarde box running *Secure Mail Suite* this will follow the format*:*

dc=machine_name,dc=domain,dc=com

Bind DN If the LDAP server requires authentication this would be the "user" it would bind to. This *Bind DN* is dependent on the LDAP server's database configuration. If the LDAP server is located on an EnGarde machine running *Secure Mail Suite* this should be set to:

cn=admin,dc=machine_name,dc=domain,dc=com

Bind DN Password This is the password that is associated with the *Bind DN*.

NOTE: The hosts IP must be listed for LDAP under *System Access Control* found in the *Security* section of the WebTool. Information regarding *System Access Control* can be found in *section 4.6.5* on page *144* of the EnGarde User Manual.

Aliases in LDAP If this option is set to *Enabled,* Postfix can lookup aliases in the LDAP database. As well as in the local alias databases.

Alias Search Order This option sets the priority search order that Postfix will use to find aliases. *LDAP* refers to the LDAP server and *files* refer to a file hash located on the local computer. Alias lookups can be configured in one or more local or remote LDAP databases.

Virtual Domains in LDAP If this option is set to *Enabled* Postfix can lookup its virtual domain configurations in the LDAP database as well as in local virtual domain databases.

Virtual Domains Search Order This option sets the priority search order that Postfix will use to find aliases. *LDAP* refers to the LDAP server and *files* refer to a file hash located on the local computer. Virtual domain lookups can be configured in one or more local or remote LDAP databases.

Once all configuration changes are made click the *Save LDAP Configuration* to save and apply the changes. Use the *Reset LDAP Configuration* button to reset everything to the factory defaults.

6.4.2 LDAP Aliases

The *LDAP Aliases* are normal e-mail aliases stored in the LDAP server. Using an LDAP server to store these aliases is faster and more efficient when working

with hundreds of aliases. It also provides consistency across multiple mail servers since they can all share the same LDAP directory of aliases.

Creating, editing and deleting LDAP aliases works the same as creating basic aliases found in *Section 6.3.1* on page *35*.

6.4.3 LDAP Virtual Domains

Like the *LDAP Aliases* above *LDAP Virtual Domains* are normal e-mail virtual domains stored in an LDAP server. An LDAP server would be used for virtual domains for the same reasons mentioned above.

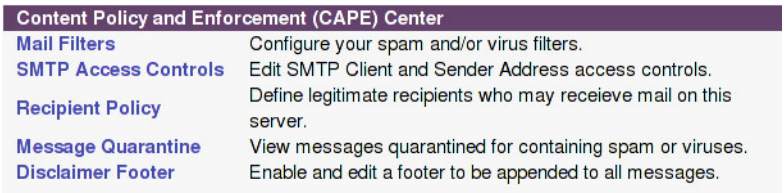
Also like the *LDAP Aliases*, *creating*, *editing* and *deleting* of the LDAP virtual domains are the same as the non-LDAP virtual domains found in the *Basic Configuration* under *Section 6.3.2* on page *38*.

7 Content Policy and Enforcement (CAPE) Center

The *Content and Policy Enforcement (CAPE) Cente*r provides proactive protection from unsolicited commercial email, offensive content, viruses, and enforcement of corporate email policies.

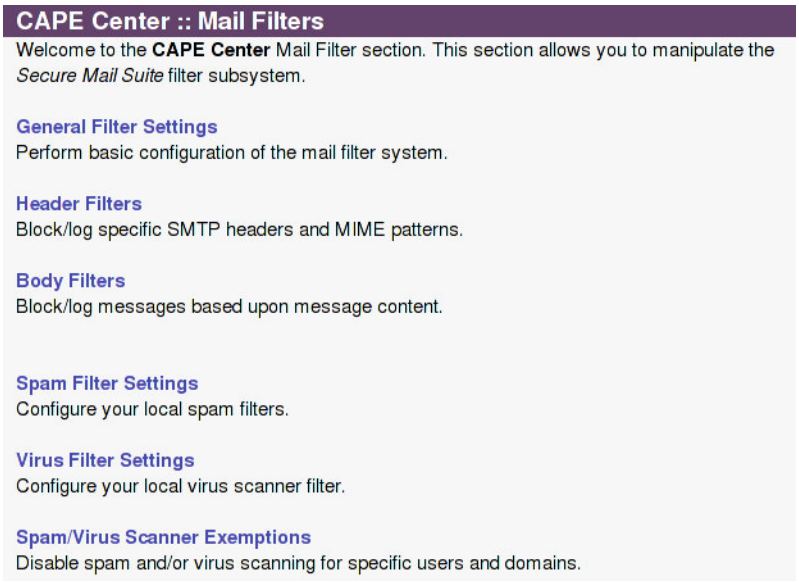
This subscription-based service can be enabled by contacting your Guardian Digital representative or visiting the Guardian Digital corporate website.

The *Content and Policy Enforcement (CAPE) Center* section covers *Mail Filters, SMTP Access Controls*, *Recipient Policy, Message Quarantine* and *Disclaimer Footer.*


Content Policy and Enforcement (CAPE) Center
Mail Filters
Configure your spam and/or virus filters.
SMTP Access Controls
Edit SMTP Client and Sender Address access controls.
Recipient Policy
Define legitimate recipients who may receieve mail on this server.
Message Quarantine
View messages quarantined for containing spam or viruses.
Disclaimer Footer
Enable and edit a footer to be appended to all messages.

7.1 Mail Filters

This section allows configuring the *Mail Filtering* subsystem of the *CAPE Center*. Here you can adjust virus/spam filters and set up email filtering based on message body and header content.

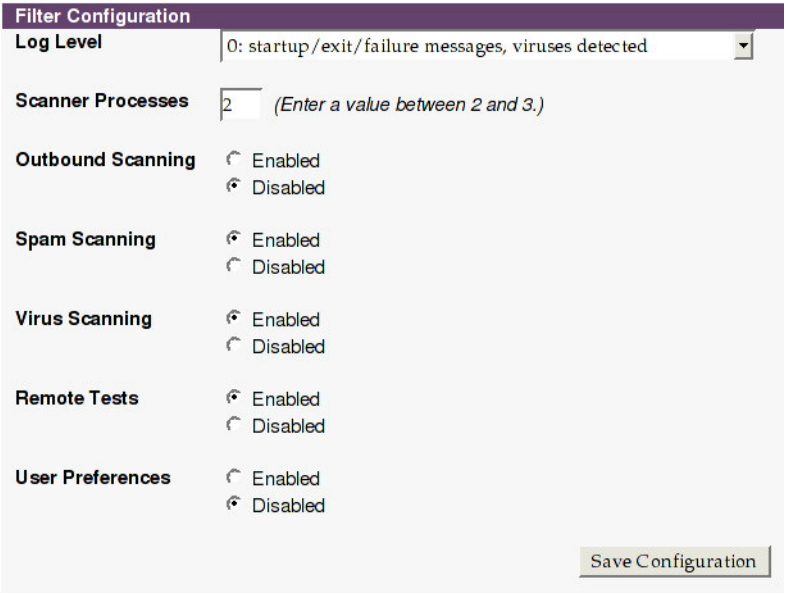

CAPE Center :: Mail Filters
Welcome to the CAPE Center Mail Filter section. This section allows you to manipulate the Secure Mail Suite filter subsystem.
General Filter Settings
Perform basic configuration of the mail filter system.
Header Filters
Block/log specific SMTP headers and MIME patterns.
Body Filters
Block/log messages based upon message content.
Spam Filter Settings
Configure your local spam filters.
Virus Filter Settings
Configure your local virus scanner filter.
Spam/Virus Scanner Exemptions
Disable spam and/or virus scanning for specific users and domains.

7.1.1 General Filter Settings

You can perform basic configuration of the mail filtering subsystem on this section. This section contains *Filter Configuration, Subject Tagging, Attachment Handling*, and *Resource Limits*.

Filter Configuration

Here you can configure basic filter settings. You can enable or disable virus and spam scanning in this section.



Log Level The verbosity of log messages. Select a value from the drop down list. If the log level is 0 only startup/exit/failure messages and messages about detected virus would be included in the logs. Setting this value to a higher number will result in more verbose and informative messages in the logs. You can view the logs in the *SMS Control Panel* in the *Maintenance and Monitoring* subsystem of the *Secure Mail Suite*.

Scanner Processes Number of scanners to run in parallel. Having more processes will increase the ability of the scanner to handle more messages at a time. However, increasing the scanner processes will result in larger usage of system resources. Recommended value is 2. For a mail server handling large volume of traffic, set this to 3.

Outbound Scanning If enabled, mail going out from this server will be scanned for virus and spam. If disabled, outgoing mail will not be scanned. If this option is enabled, you can create whitelists for domains exempted from ourboud spam scanning. Refer to section 7.1.4on page 71for more information about outbound domain whitelists.

Spam Scanning Enable or disable spam scanning. If enabled, email passing through this server will be scanned for the possibility of being bulk mail

(spam). More advanced configuration of the spam filtering subsystem can be done in the *Spam Filter* section of *Mail Filters* (page 55).

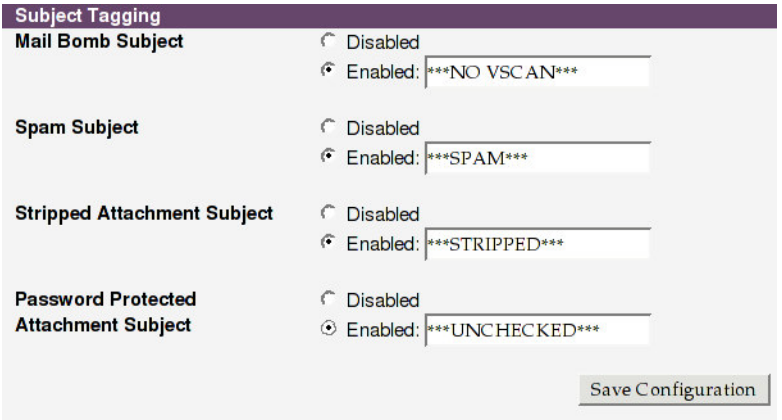
Virus Scanning Enable or disable virus scanning. If enabled, email passing through this server will be scanned for viruses. More advanced configuration of the virus scanner can be done in the *Virus Filter* section in *Mail Filters* (page 74).

Remote Tests The spam scanning subsystem makes use of certain servers on the Internet while determining if a message is spam or not. These include *Real-time Black-hole List (RBL)* tests and *Distributed Checksum Clearinghouse (DCC*) checks. If remote tests are disabled, no test that needs Internet access will be performed by the spam scanner. Disabling remote tests may improve the system performance if the server is behind a firewall and can't contact outside servers, but may affect the efficiency of the spam scanner.

User Preferences *Secure Mail Suite* allows local users to set up their own filter settings. Here you can enable or disable this functionality. If enabled, individual users will be allowed manipulate how to filter email addressed to them.

Subject Tagging

The mail filter can add tags to the subject of the messages that it has identified as illegitimate or harmful. These tags will be prepended to the subject of mail passing through the filter so the recipient can identify or classify the messages easily. You may enable/disable subject tagging and change the tags.



Mail Bomb Subject The subject tag for mail bombs. The mail filter will open archive files in attachments (Eg: ZIP files) before scanning them for viruses. Mail bombs are certain malicious archive files which expand to a very large size while opening, making it impossible to scan them. These mail bombs are intended to choke mail filters. The *Secure Mail Suite* can detect mail bombs and attach a tag to the subject of these mails.

Spam Subject Subject tag for mail identified by the filter as bulk mail (spam). If disabled, no tags will be attached to the mail. To enabled tagging, select *Enabled*, and enter the tag in the box.

Stripped Attachment Subject Subject tag for mail from which attachments were removed by the mail filter. Attachment handling can be configured in the section below.

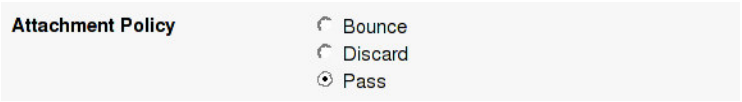
Password Protected Attachment Subject Certain viruses come in attachments that are zipped with a password. The password is usually mentioned in the body of the mail. Usually, the recipient may be tempted to open the zip file supplying this password, causing infection. Opening the password protected attachments from the scanner is almost impossible, making it very difficult to scan them for viruses. Here you can specify a subject tag for mail which are unchecked due to a password protected attachment.

Attachment Handling

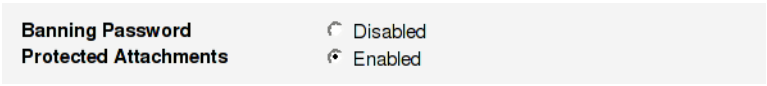
This section allows you to configure attachment filtering. The following settings control how e-mail attachments are handled by the mail server.

Attachment Policy Attachment policy defines what action will be performed when an email containing a banned attachment is received. If the email attachment matches the criteria set by *Strip Behavior* and *Attachment Extensions* options described below, the attachment policy will be performed. If *Bounce* is selected, the message is not delivered to the recipient and sender is notified. If *Discard* is selected, the message is not delivered and the sender will not be notified. If *Pass* is selected, the message and the attachment is delivered to the recipient.

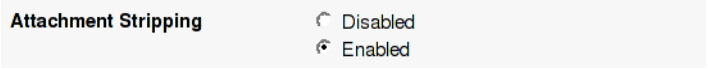
Attachment Stripping should be disabled for *Attachment Policy* to take effect. This option also determines the destiny of mail containing undecipherable attachments, if they are banned in the option below (*Banning Undecipherable Attachments*).



Banning Password Protected Attachments Here you can block email that contain password protected files (files zipped with a password). Password protected attachments cannot be opened and checked for viruses reliably, so it is a good idea to ban them. This option will take effect only if *Attachment Stripping* (described below) is disabled, and *Attachment Policy* (described above) is set to *Bounce* or *Discard*. If this option is enabled, then mail containing password protected attachments will be subjected to *Attachment Policy* (described above).

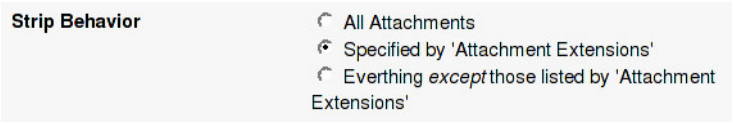


Attachment Stripping If enabled, the email attachments matching the criteria defined by *Strip Behavior* and *Attachment Extensions* options will be removed from the mail, and the rest of the mail is delivered to the users. Enabling *Attachment Stripping* takes precedence over *Attachment Policy*. If *Attachment Stripping* is enabled, the *Attachment Policy* option described above will not take effect.



Strip Behavior This option allows you to define banned attachments.

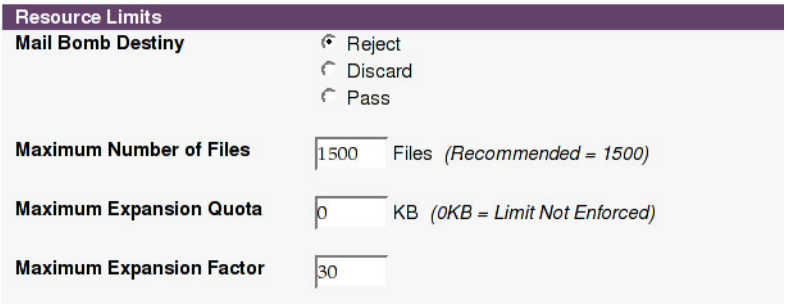
- **All Attachments** All attachments are banned.
- **Specified by Attachment Extensions** Only those attachments whose extension is specified in *Attachment Extensions* section will be banned.
- **Everything except those listed** All attachments with extensions that are not listed in the *Attachment Extensions* section below will be banned. Only those attachments with extensions listed in *Attachment Extensions* section will be allowed.



Attachment Extensions Enter attachments extensions in this field. The attachments whose extensions match those listed here will be banned or exempted from banning, depending on the settings above. Extensions should be separated by spaces. More than one attachment extension can be entered on a line.

Resource Limits

In this section you can define settings for detecting mail bombs. Mail bombs are compressed email attachments, such as a zip file, which expands to a very large size when decompressed. The mail scanner opens compressed archives before scanning them, so trying to scan a mail bomb may use system resources indefinitely, choking the mail filtering system. Below, you can define the settings for detecting mail bombs and their destiny. If any of the three limits described below is exceeded while opening an archive attachment, the filter will not try to open the archive further and detect the mail as a mail bomb.



Mail Bomb Destiny Here you can set the destiny of emails that contains mail bombs.

- ***Bounce*** Do not deliver messages containing mail bombs. Notify the sender.
- ***Discard*** Do not deliver messages containing mail bombs. Do not notify the sender.
- ***Pass*** Messages containing mail bombs should be delivered to the recipient.

Maximum Number of Files Mail bombs usually contain very large number of files. Here you can define the maximum number of files permitted in an attached archive file. If the number of files in the archive is greater than this number, the mail is detected as a mail bomb.

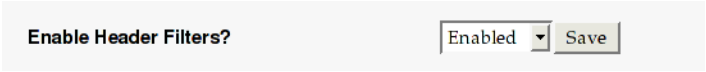
Maximum Expansion Quota Maximum size of an archive file after expanding, in kilobytes. If an attachment exceeds this size limit when uncompressed, it is detected as a mail bomb. If 0 is entered, the limit is not enforced.

Maximum Expansion Factor *Expansion factor* is the ratio of the size of the decompressed archive to the original uncompressed archive file. This limit is exceeded when the decompressed archive gets larger than the original attachment by this factor. Default value is 30, which means if the size of the extracted file is 30 times the original file, the *Mail Bomb Destiny* will be performed for this file.

7.1.2 Header Filters

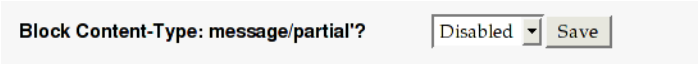
Header Filters allows specific headers to be filtered out from being sent. This is primarily used for blocking spam and viruses.

Header Filters is disabled by default. From the pull-down menu select *Enabled* and then click the *Save* button to enable *Header Filter*s. Once it is enabled, the option *Block Content-Type: message/partial* will be displayed.



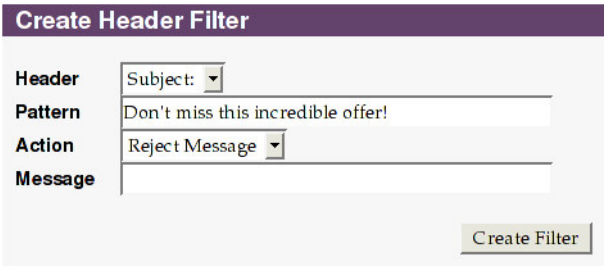
Message/partial is a specific MIME type which allows a single object to be split in to different pieces and delivered in separate mail, to be reassembled at the

recipient. Since each mail will have only a fraction of the original message, it is not possible to scan messages with this MIME type. These messages are normally malicious and you can block this particular MIME type by enabling the option below.



Creating Header Filters

The *Header Filters* will be used to determine if an e-mail matching a pattern will be delivered and logged or rejected. To create a new *Header Filter,* click *Define New Header Filter*.



Header A *Header* must be chosen for the filter. The pull-down menu contains the options *To*, *From*, *Subject* and *CC*. The pattern specified in the *Pattern* field will be searched only in the header field specified here.

For example, if *From* is chosen for the header and a pattern of *john.doe@domain.com* then any e-mail sent with a *From:* field that matches *john.doe@domain.com* will be caught by this pattern.

Pattern This is the search pattern to be used for this header check. The pattern does not need to be the complete string but only a portion of it to make a match. For example, "great offer" might have also been used. If the *Header*, described above, is set to *Subject* then any e-mail where the subject contains "great offer" will be flagged.

Action When an e-mail matches the pattern it will take action against it. The pull-down menu contains the options *Reject Message* and *Log Warning*.

Log Warning allows the e-mail to be delivered to its destination but it will be logged.

Reject Message will deny the message completely.

Message When an e-mail matches the pattern and the action is taken, the contents of this *Message* field will be used in response. If *Log Message* was chosen as the *Action* then this message will be stored in the logs. If *Reject Message* was chosen as the *Action* then this message will be sent to the sender of the message, and stored in the logs.

This *Message* field is not required to create the pattern.

Once all the fields are completed click the *Create Filter* button. The new header filter will appear in the list. Filters configured to reject the message are highlighted in red, filters set to only log the message are highlighted in green.

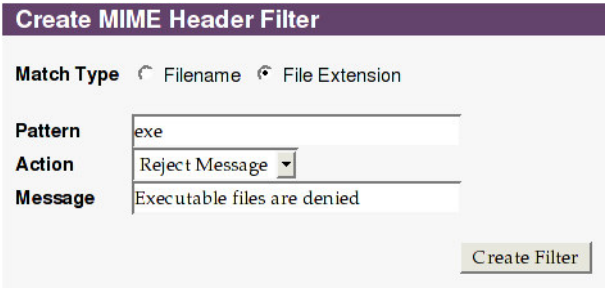
The order the filters are listed in is also their priority order. To change the priority of a listed filter select the up or down arrow to the right of the filter to move it up and down through the list.

To edit or delete a filter, click on the *Edit* link to the left of the pattern. This will open a new window displaying the filter's information. Make changes and click *Update Filter* or choose to delete the filter by clicking the *Delete Filter* button.

MIME Header Filters

The *MIME Header Filters* will search e-mail attachments for specific patterns. This will search the attachment by filename or file extension and has the ability to block the e-mail or log and deliver it.

To create a *MIME Header Filter* click the fine *Define New MIME Header Filter* link. A new window will appear with the option to create the pattern.



Match Type The chosen pattern will be matched against either the *Filename* or the *File Extensions*.

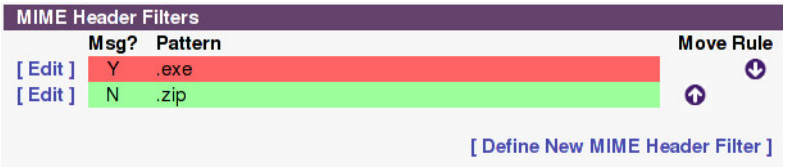
Pattern This is the pattern that will be used to match against the *Match Type*. A complete filename or just the extension can be entered here.

Action When an e-mail matches the pattern it will take action against it. The pull-down menu contains the options *Reject Message* and *Log Warning*.

Message When an e-mail matches the pattern and the action is taken, the contents of this *Message* field will be used in response. If *Log Warning* was chosen as the *Action* then this message will be stored in the logs. If *Reject Message* was chosen as the *Action* then this message will be sent to the sender of the mail and stored in the logs.

This *Message* field is not required to create the filter.

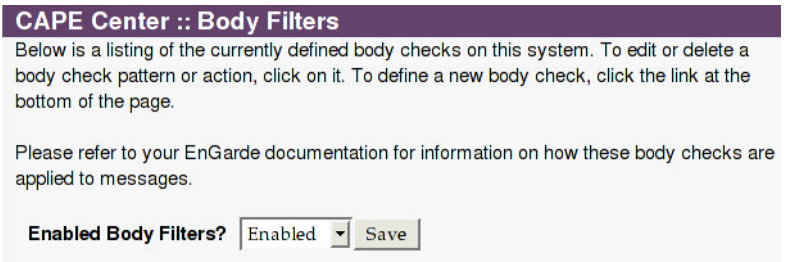
Once all the fields have been completed click *Create Filter* to create the filter. Once created, the filter will appear on the menu under *MIME Header Filters*. As with the *Header Filters* mentioned earlier, the *MIME Header Filters* are listed in the order of their priority. Filters configured to reject e-mails will be highlighted in red and filters configured to only log them will be highlighted in green.



To edit or delete a pattern click the *Edit* link located to the left of the filter. This will open a new window displaying the content of the pattern. Changes can be made to this and saved by clicking the *Update Filter* button. It can be deleted by clicking the *Delete Filter* button.

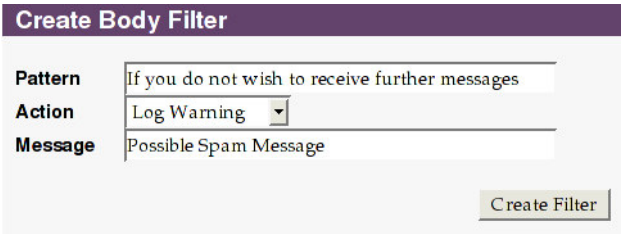
7.1.3 Body Filters

Body Filters search the body of an e-mail for a specified pattern. If the pattern matches something in the body, the specified action is taken.


CAPE Center :: Body Filters
Below is a listing of the currently defined body checks on this system. To edit or delete a body check pattern or action, click on it. To define a new body check, click the link at the bottom of the page.
Please refer to your EnGarde documentation for information on how these body checks are applied to messages.
Enabled Body Filters?
Enabled
Save

Body Filtering is disabled by default. From the pull-down menu select *Enabled* and then click the *Save* button to enable *Body Filter*s. Once it is enabled, *Body Filters* can be created as described below.

To create a new *Body Filter* click the *Define New Body Filter* link.



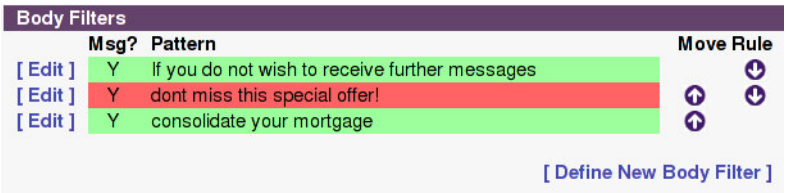
Pattern This is the pattern text to search for in the body of the e-mail. If this pattern is found the specified action will be taken.

Action Upon finding the pattern specified above, an action will take place. Here is a pull-down menu to choose to *Reject the Message* or *Deliver and Log Warning*.

Message When an e-mail matches the pattern and the action is taken, the contents of this *Message* field will be used in response to the sender. If *Log Warning* was chosen as the *Action,* this message will be stored in the logs. If *Reject Message* was chosen as the *Action,* this message will be sent to the sender of the mail and will be stored in the logs.

This *Message* field is not required to create the filter.

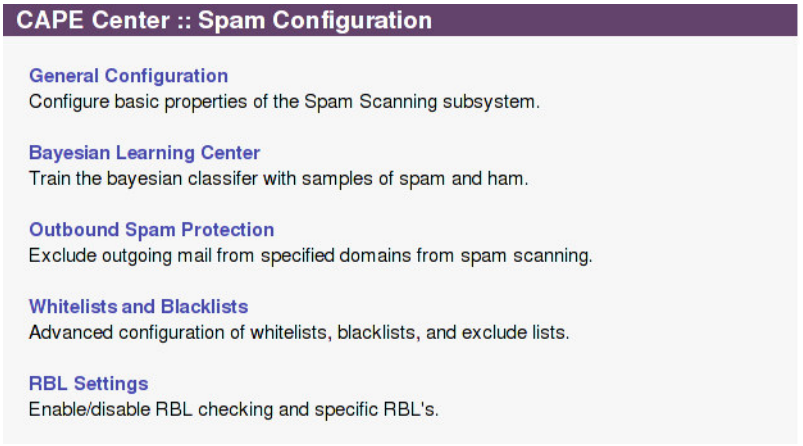
Once all the fields have been completed click *Create Filter* to create the filter. Once created, the filter will appear on the menu under *Body Filters*. As with the *Header Filters* mentioned earlier, the *Body Filters* are listed in the decreasing order of their priority. Filters configured to reject e-mails will be highlighted in red and filters configured to only log them will be highlighted in green.


Body Filters
Msg? Pattern
Move Rule
[Edit] Y If you do not wish to receive further messages
[Edit] Y dont miss this special offer!
[Edit] Y consolidate your mortgage
[Define New Body Filter]

To edit or delete a pattern click the *Edit* link located to the left of the filter. This will open a new window displaying the content of the filter. Changes can be made to this by clicking the *Update Filter* button and can be deleted by clicking the *Delete Filter* button.

7.1.4 Spam Configuration

Secure Mail Suite allows detailed configuration of the *Spam Scanning* subsystem. The *Spam Configuration* menu options allow fine tuning of the spam filtering process. Here you may set up thresholds for detecting the spam, different spam destinies, *Bayesian Filtering*, whitelisting and blacklisting, RBL etc.

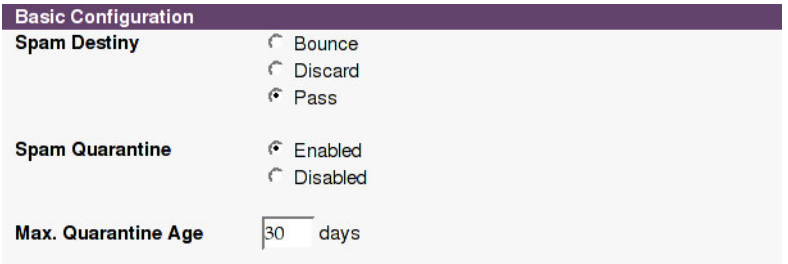

CAPE Center :: Spam Configuration
General Configuration
Configure basic properties of the Spam Scanning subsystem.
Bayesian Learning Center
Train the bayesian classifer with samples of spam and ham.
Outbound Spam Protection
Exclude outgoing mail from specified domains from spam scanning.
Whitelists and Blacklists
Advanced configuration of whitelists, blacklists, and exclude lists.
RBL Settings
Enable/disable RBL checking and specific RBL's.

General Configuration

The *General Configuration* allows configuration of the *Spam Scanning* subsystem. This section is broken down in to *Basic Configuration, Thresholds, Bayesian Configuration, Distributed Checksum Clearinghouse (DCC)* and *Advanced Configuration.*

Basic Configuration

The *Basic Configuration* has the following options:



Spam Destiny This determines the fate of an e-mail detected as spam. The *Bounce* option will reject the mail from the mail server the e-mail came

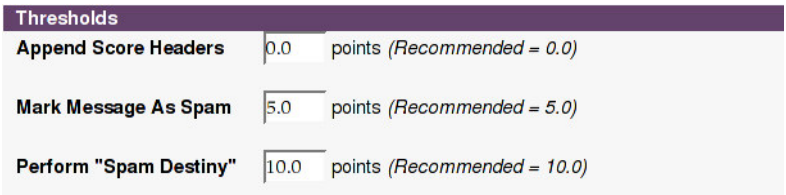
from with a response back to that server. *Discard* will just drop the message completely but acknowledge receiving the e-mail. *Pass* will send the message on to its recipient but it will be marked as spam.

Spam Quarantine When a spam message is received this will determine if the message will be quarantined. If this is *Enabled* it will always be quarantined regardless of the *Spam Destiny* setting. For example, if the *Spam Destiny* is to pass on to the recipient, a copy will be quarantined as well.

Max. Quarantine Age If *Spam Quarantine* is *Enabled* then this option will determine how many days the message will live in the quarantine. Once it is expired the message is removed from the system.

Thresholds

When the spam scanner scans the message, it calculates a score which reflects the probability that the message is spam. A message with a high score is more likely to be a spam than a message with a lower score. The spam scanner will mark a message as spam if its score is greater than the threshold. In this section, you can define the score threshold for particular actions to be taken on the message.



NOTE: It is important to make small incremental changes at a time, as large changes may adversely impact performance.

Append Score Headers If the score of the message is greater than this threshold, a descriptive header is attached to the header of the message. The message will be delivered, without marking it as spam. The score headers are for informational purposes only. By looking at the score headers, one can see which of the various spam tests succeeded on this message. The recommended value is 0.

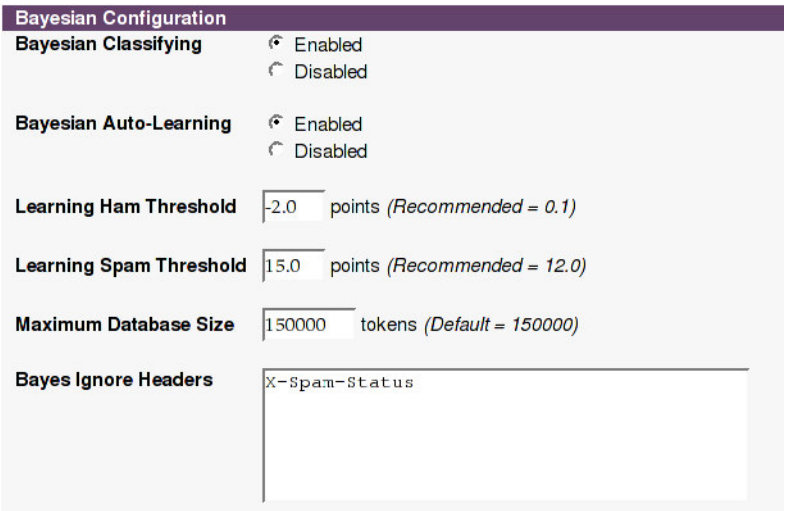
Mark Message As Spam If the score of the message is greater than this threshold, the message is marked as spam and is delivered to the recipient. The

delivered message will have the spam subject tag. If the *Spam Scanning* is catching too many non-spam e-mail, raise this number. If too many spam messages are getting through undetected, try lowering this number.

Perform Spam Destiny If the score of the e-mail exceeds this threshold, the message is subjected to the *Spam Destiny* defined in the *Basic Configuration* section above. Depending on the *Spam Destiny*, the message will be *bounced*, *discarded* or *passed* to the recipient.

Bayesian Configuration

Bayesian Classification is a method by which the spam scanning system learns about what is considered spam and what is not. It works by keeping a database that contains the probability that a message containing a particular word is spam. When it scans a new message, the Bayesian filter employes a heuristic method to calculate the probability the message is spam, from the individual probabilities of the words in the message. Since the Bayesian filter solely depends on the information it has learned from the previous messages, it is very important to keep the Bayesian database updated by constantly teaching it using spam and non-spam messages. Bayesian filtering has a very significant effect on the efficiency of the spam scanning subsystem.



Bayesian Classifying You can enable or disable *Bayesian Classifying* here. It is

highly recommended that you enable this option. Enabling *Bayes Classifying* can drastically improve the performance of spam filtering.

Bayesian Auto Learning The Bayesian filter will learn automatically from messages passing through the filter, once it is manually seeded with a minimum of 200 ham and 200 spam messages. Manually seeding the Bayesian database is discussed in the *Seeding Bayes Database* section, in the *Bayesian Learning Center* on page 65. Since it needs no human intervention afterwords, it is a very convenient way to train the Bayesian filter. It is recommended that this option is enabled.

Learning Ham Threshold This threshold is used to determine if a message should be learned by the Bayesian filter as a legitimate message (ham). If the spam score of a message is less than this threshold, the Bayesian filter will learn this message as a legitimate message. This score should be a very low number, close to zero, to make absolutely sure this message is legitimate and the Bayesian filter doesn't learn any spam messages as ham.

Learning Spam Threshold This threshold is used to determine if a message should be learned by the Bayesian filter as a spam message. If the score calculated from the message is greater than the value specified here, the message will be learned as spam. This number should be set to a high value to make absolutely sure that the message is indeed spam. Setting this to a low value may result in some legitimate mail getting learned as spam, which will adversely affect the efficiency of the spam scanner.

Bayes Ignore Headers Here you can enter the mail headers that the Bayesian filter will not learn. If the received mail is already filtered by another mail system, like a spam filtering ISP, or mailing list, they may add certain headers in the message. These headers may provide unnecessary clues to the Bayesian filter when it learns those messages, which may result in the filter developing a tendency to give more importance to these headers than the contents of the message.
Eg: X-Spam-Status

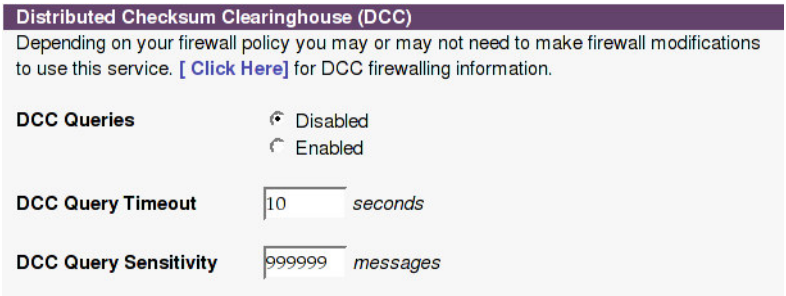
Distributed Checksum Clearinghouse (DCC)

The *Distributed Checksum Clearinghouse or (DCC)* is a cooperative, distributed system intended to detect *bulk* mail or mail sent to many people. It allows individuals, receiving a single mail message, to determine that many other people have received essentially identical copies of the message and thus to reject or discard the message.

There are a group of servers on the Internet that maintain a database of reported mail by other DCC users. When the mail server receives an email it calculates a checksum of that email and sends this value to one of the DCC servers. The DCC server will then store this checksum and look through its database and return a count of how many emails it has already stored from other DCC users that closely match this checksum. If this email matches a high number of emails that have already been stored then it is considered *bulk* email. Based on a threshold that SMS users sets, this email will accrue a spam score.

DCC is a network based service, so the *remote tests* option should be enabled in Mail Filters :: General Filter Settings :: Filter Configuration for DCC to work.

NOTE: No confidential information of any kind is transmitted to the DCC servers.


Distributed Checksum Clearinghouse (DCC)
Depending on your firewall policy you may or may not need to make firewall modifications to use this service. [Click Here] for DCC firewalling information.
DCC Queries
Disabled
Enabled
DCC Query Timeout
10
seconds
DCC Query Sensitivity
999999
messages

DCC Queries You can enable or disable DCC checking. It is highly recommended that you enable DCC.

DCC Query Timeout A query to the DCC server gets timed out after this many seconds. If the DCC server doesn't respond to queries even after this time period, the DCC test is dropped and the filter proceeds with other tests.

DCC Query Sensitivity This setting is the threshold by which the email in question will receive spam points if the returned count from a DCC server is crossed. The default setting is 50000. In other words there needs to be at least 50000 emails reported to DCC by other DCC users that match the check sum of the email being filtered before it receives extra spam points. Setting this to a lower number will increase the sensitivity of the DCC test. Keep in mind that setting this to a very small number (<1000) may block legitimate mailing list messages since mail from mailing lists are sent to a large number of users and could have a large count in the DCC databases.

Distributed Checksum Clearinghouse (DCC) is a network-based service. In order to use DCC your *Secure Mail Suite* server must be able to communicate with *DCC servers* over UDP port 6277. There are two ways to ensure this communication. The first method is to configure your firewall to permit traffic to and from any external host over 6277/udp.

The second method is to only open up your firewall to valid DCC servers. This list changes every so often so this is not the preferred method. However if your company has a stringent firewall policy this may be your only option.

Visit *http://infocenter.guardiandigital.com/dcc* for a list of IP addresses used by the DCC servers.

The Advanced Configuration

The *Advanced Configuration* section allows fine tuning of the spam filtering capabilities. Generally this should be left alone and the system will work fine. The options are explained below.

Full Header Reporting If enabled, the spam filter will append detailed information about the scanning results in the header of the email message. This information is useful for debugging those messages that the spam filter missed.

Max Message Size to Spam Scan Scanning a message for spam takes up a lot of system resources. If the message has a very large size, too much time may be spent analyzing the message. Here you may specify the maximum size of the message that are scanned for spam. If an email is larger than this

amount in kilobytes, that message is not scanned for spam. Spam typically isn't larger than 150K.

RBL Lookup Timeout Real-time Black-hole List (RBL) are servers on the Internet that keep a database of machines and domains that regularly send spam. The spam scanner contacts RBL if that option is enabled. Here you can specify the timeout in seconds for contacting the RBL servers. If the scanner doesn't receive a reply from an RBL server after this many seconds, it drops the RBL checks.

Local Languages The *Spam Scanning* will not assign a spam point value for being in a foreign language for each language selected here. More than one *Local Language* can be set.

Local Character Sets As with the *Local Languages* above if an e-mail is sent in a character set not defined as a *Local Character Set* it will be assigned a spam point value.

Bayesian Learning Center

The following describes the steps to teach the Bayesian Classifier in spam recognition. This section is accessed by clicking *Bayesian Learning Center* from *Mail Filters :: Spam Configuration*. The purpose of this section is to help you keep the Bayesian filter updated, so that it can recognize constantly evolving spam.

See the end of this section for a summary on instructions for keeping Bayesian database updated.

What is Bayesian Classifying?

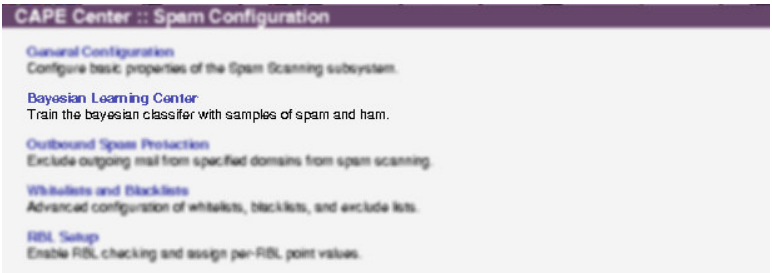
Given training, a spam heuristics engine can take the most *spammy* and *hammy* words and apply probabilistic analysis. Furthermore, once given a basis for the analysis, the engine can continue to learn iteratively by applying both its Non-Bayesian and Bayesian rule set together to create evolving *intelligence*.

Using a classifier such as this drastically increases the effectiveness of *Guardian Digital Secure Mail Suite*. It is highly recommended that you enable and use this feature.

Before you may use the *Bayesian Classifier* you must configure and train it to recognize spam (unsolicited email) and ham (the opposite of spam – legitimate email). Below is a discussion of the former, and the next section is a discussion of the latter.

Database Maintenance

The following documentation describes the steps to teach the Bayesian classifier in spam recognition. The Bayesian classifier can be used on either an email storage server (where email recipients have local accounts) or on an email gateway. The difference in operation will be discussed later.


CAPE Center :: Spam Configuration
General Configuration
Configure basic properties of the Spam Scanning subsystem.
Bayesian Learning Center
Train the bayesian classifier with samples of spam and ham.
Outbound Spam Protection
Exclude outgoing mail from specified domains from spam scanning.
Whitelists and Blacklists
Advanced configuration of whitelists, blacklists, and exclude lists.
RBL Setup
Enable RBL checking and assign per-RBL point values.

Learning Spam and Ham

Definitions:

Spam: Unsolicited commercial email

Ham: Valid email

False Positive: A valid email that was erroneously classified as spam

False Negative: A spam email that was erroneously classified as valid

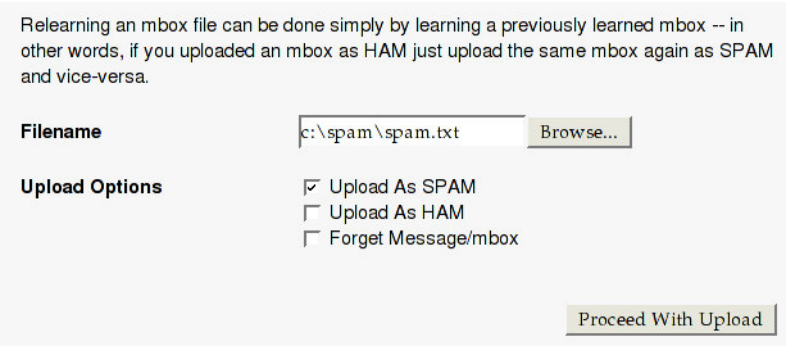
The role of the *Bayesian Classifier* is to put incoming email into 3 categories - *spam, ham* and *not-sure* (not-sure is a mail that isn't clearly spam or ham and therefore is not auto-learned as either). It does this by breaking incoming mail into *tokens*. Tokens are mostly words found in the email body but are also elements of the email headers and envelope. It then determines how often these tokens occur in spam and ham (based on what it has been previously taught). With this information it can then add spam points to an incoming email as necessary to enhance the total spam filter's spam detection capability. So the first step is to initialize or *seed* the Bayes database which has to be done before it can be used. There are two ways in which the admin can teach spam and ham into the Bayes database. One is by uploading spam and ham *mbox* files and the other is to learn from local users. Visit *http://infocenter.guardiandigital.com* to get more information about mbox files.

NOTE: Learning from local users can only be done on an email server where the recipients have local accounts on the server. This is the difference between gateway operation and a server that stores email. Only the storage server can be used for this function.

Seeding the Database

The *Bayes Classifier* won't even start running until it has learned a minimum 200 spam and 200 ham emails. This means that ham is just as important as spam and an equal balance is needed for optimal performance. Seeding requires the preliminary collection at least 200 known spam and 200 known ham messages. Feel free to seed the database with larger amounts of spam and ham (in approximately equal amounts of both). The more samples it is seeded with the better its initial performance will be. Store all of the spam in one file in the *mbox* style format. Do the same with all of the ham. Spam and ham needs to be put in separate files before being fed to Bayes.

Once that is done and these files have been transferred to the machine where the admin is running the WebTool from she can upload these files onto the machine that is running the *Secure Mail Suite* spam filter using the *Bayesian Classifier.* This is done in the *Upload Ham/Spam Mailbox* section of the WebTool page mentioned above. There is a *Browse* button which allows the admin to upload the spam and ham files separately. Choose one of three upload options, *Upload as SPAM, Upload HAM* or *Forget Message/mbox*. (The *Forget* option will be discussed later). After making the proper choice click on the *Proceed With Upload* button. Do this for both the spam and ham *mbox* files.


Relearning an mbox file can be done simply by learning a previously learned mbox -- in other words, if you uploaded an mbox as HAM just upload the same mbox again as SPAM and vice-versa.
Filename
c:\spam\spam.txt
Browse...
Upload Options
Upload As SPAM
Upload As HAM
Forget Message/mbox
Proceed With Upload

NOTE: These files MUST have world read permissions OR THEY WILL NOT BE LEARNED! If they are not world-readable, change their permissions to 644

as the *root* user if necessary. You need to actually log onto the server where the files reside, in the root shell account, to do this.

This will generally take from a couple of seconds to a minute or so depending on the file size. An easy way to verify if that the files were successfully learned is by observing the *Bayes Database Statistics* section at the bottom of the page. Click on your browser's *Reload* button to ensure that the web page has been updated. You will see the some database statistics including the number of spam and ham emails that it has learned. Once these values are greater than 200 for both spam and ham the database can be used to classify and auto-learn incoming mail. (The auto-learn feature is described on page 69 of this guide).

Re-Learning Email

In the event that the admin has erroneously learned a spam file as ham and vice-versa, don't worry. The admin can browse this file again and relearn it. For example, if *c:\spam\message.txt* was learned as ham by accident it can be learned as ham by browsing the same file, checking the *Upload as SPAM* box and clicking on *Proceed With Upload*. You will then see that the ham count will have been reduced by the number of spam emails contained in *c:\spam\message.txt* and the spam count will have been increased by this same number.

Forgetting Previously Learned Email

If for some reason an admin later determines that a previous file should not be contained in the database as spam or ham she can tell the database to remove the associated tokens entirely by browsing the file once more, checking the *Forget Message/mbox* box and clicking on *Proceed With Upload* button. Once again the Bayes database statistics will reflect the removal.

Learning From Local User's Email

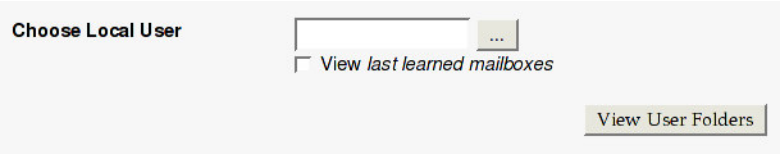
NOTE: This can only be done on an email server that stores the local user's email. THIS CANNOT BE DONE ON AN EMAIL GATEWAY.

The second way in which spam and ham can be learned is by local user contributions. The requirements are that the users have IMAP accounts on the server and that they create two top level folders (folders that are in the same folder hierarchy as the INBOX folder). These folders MUST BE named "SPAM" and "HAM"

(capital letters are NECESSARY). Once this is done users can copy or move their false negatives into the "SPAM" folder and their false positives into the "HAM" folder.

NOTE: CHOOSE THESE USERS WITH CARE! Trusting careless or malicious users can poison the Bayes database. If the user contributes ham as spam or vice-versa, the database will operate on erroneous data and will result in operation that ranges anywhere from poor performance to reversal of email classification.

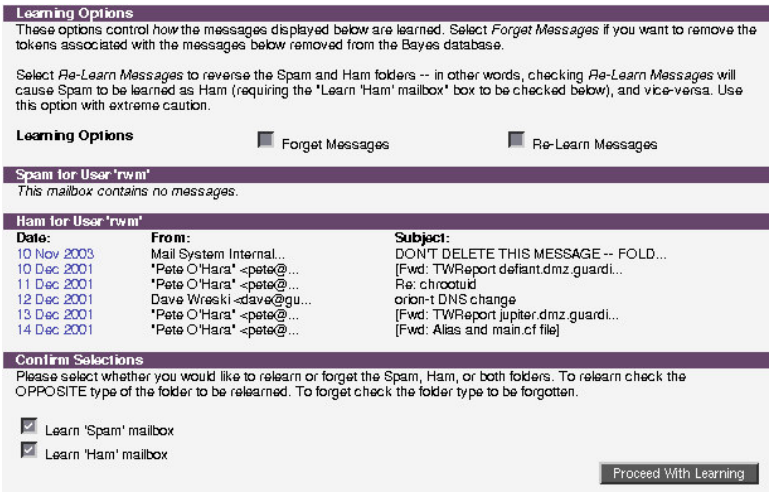
Once a user has deposited spam and ham into the appropriate folders the admin can learn these folders into the Bayes database in the *Learn Users Spam/Ham Folders* section of the web page. All users that have created SPAM and HAM folders can be viewed in the *Select User-Name* pull down menu.



Choose a user and click on *View User Folders*. The admin can view the email and decide whether to learn it or not. If there are any doubts as to whether the email is suitable for the database then no learning is accomplished by backing out this web page or by unselecting the appropriate check-box of *Learn SPAM mailbox* or *Learn HAM mailbox*. This is useful if the admin feels that one of the folders is acceptable but not the other. For example, if the admin approves of the SPAM folder but not the user's HAM folder she can unselect the checkbox next to *Learn HAM mailbox* and proceed with the learning. In this way only the SPAM folder will be learned. Only entire folders can be learned. The admin cannot selectively choose email within a folder. Once again the results of the learning can be verified by viewing the spam, ham and token counts in the statistics section of the *Bayesian Learning Center* web page.

If an admin feels that she has made a mistake in learning a user's email she can relearn or forget the previously learned email by choosing the user, checking the *View last learned mailboxes* check-box and clicking on *View User Folders*. A list of the most previously learned mail will be available. To relearn the email the admin can check the *Re-Learn Messages* checkbox. Additionally, in the *Confirm Selections* section of the web page the admin has to select a check-box that represents the OPPOSITE type of the folder being relearned. Another way to think of it

is to check the type of classification that will be the END RESULT of the learning. For example if the user's HAM folder was previously learned as spam by mistake the admin should see this mail now represented as spam. She would then check *Re-Learn Messages* and *Learn HAM mailbox* and click on *Proceed With Learning* to relearn the email as ham.

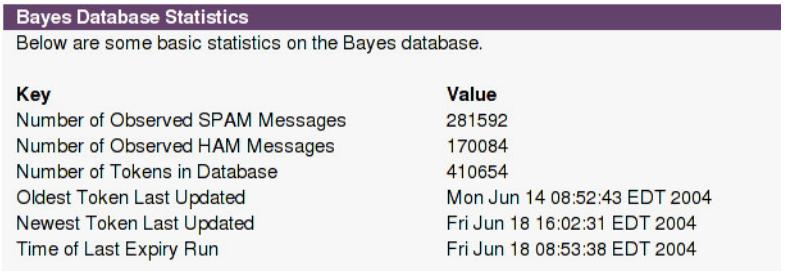

Learning Options
These options control how the messages displayed below are learned. Select Forget Messages if you want to remove the tokens associated with the messages below removed from the Bayes database.
Select Re-Learn Messages to reverse the Spam and Ham folders -- in other words, checking Re-Learn Messages will cause Spam to be learned as Ham (requiring the "Learn 'Ham' mailbox" box to be checked below), and vice-versa. Use this option with extreme caution.
Learning Options
Forget Messages
Re-Learn Messages
Spam for User 'rwm'
This mailbox contains no messages.
Ham for User 'rwm'
Date: From: Subject:
10 Nov 2003 Mail System Internal... DON'T DELETE THIS MESSAGE -- FOLD...
10 Dec 2001 "Pete O'Hara" <pete@... [Fwd: TWReport defiant.dmz.guardi...
11 Dec 2001 "Pete O'Hara" <pete@... Re: chrootuid
12 Dec 2001 Dave Wreski <dave@gu... orion-t DNS change
13 Dec 2001 "Pete O'Hara" <pete@... [Fwd: TWReport jupiter.dmz.guardi...
14 Dec 2001 "Pete O'Hara" <pete@... [Fwd: Alias and main.cf file]
Confirm Selections
Please select whether you would like to relearn or forget the Spam, Ham, or both folders. To relearn check the OPPOSITE type of the folder to be relearned. To forget check the folder type to be forgotten.
Learn 'Spam' mailbox
Learn 'Ham' mailbox
Proceed With Learning

To *forget* email check the *Forget Messages* checkbox and in the *Confirm Selections* section check the appropriate checkbox that represents the folder that the admin would like to have removed entirely from the database.

Maintaining the Database

Now that the database is seeded, it needs to be maintained. This encompasses auto-learning, relearning false positives and false negatives, backup and restores and viewing statistics.

Statistics The statistics are shown in the *Bayes Database Statistics* section at the bottom of the web page. They are made up of the number of spam and ham that has been seen by the database since its beginning. It also shows the number of tokens that are currently stored in the database. This number will increase and decrease as the database learns new tokens and expires old tokens. There is also the time stamps of the oldest and newest tokens in the database and the time stamp of the last expiry run.



Bayes Database Statistics

Below are some basic statistics on the Bayes database.

Key	Value
Number of Observed SPAM Messages	281592
Number of Observed HAM Messages	170084
Number of Tokens in Database	410654
Oldest Token Last Updated	Mon Jun 14 08:52:43 EDT 2004
Newest Token Last Updated	Fri Jun 18 16:02:31 EDT 2004
Time of Last Expiry Run	Fri Jun 18 08:53:38 EDT 2004

NOTE: You may experience learning a number of spam or ham and not seeing the expected increase in database statistics. This is most likely due to the fact that the *Bayes Classifier* has already learned some of the email that you are feeding it. When this happens the spam or ham counts will only be incremented by the amounts of new email.

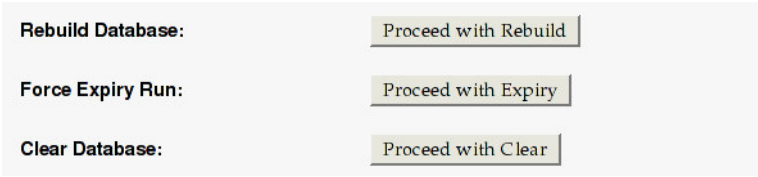
Auto-learning The *Bayesian Classifier* can automatically categorize incoming email based upon the tokens it sees within the email compared with tokens in the database. In this manner it becomes an adaptive filter automatically learning new spam. This feature is controlled in the *General Configuration* web page under *Spam Configuration*, described on page 59.

Maintaining a Balanced Spam/Ham Ratio In general, it is a good idea to keep the spam and ham counts approximately equal to give the classifier an unbiased point of view. View the spam and ham count statistics . If one gets noticeably higher than the other (somewhere around a 10% to 15% difference) it would be a good idea to adjust the *Learning Ham* and *Learning Spam* thresholds to balance the spam and ham counts. It is wise to make small adjustments to these thresholds and watch the counts over a day or two before further adjustments. It is better to see small shifts rather than large swings in the spam/ham ratio.

Learning From User Contributions You should obtain false positive and false negative messages and feed them into the Bayesian database. This provides another aspect of fine tuning the database (auto-learning being the other one). But as stated above, be extremely cautious on what users you learn from. A poisoned database defeats the purpose of having one.

Rebuilding The Database This operation rebuilds the database, performing operations such as optimizing token order. It also synchronizes the database journal with the database itself. During auto-learning data is stored in the journal instead of directly in the database. This file gets synchronized on an

automatic basis but one could do a manual sync here as well by clicking on the *Proceed with Rebuild* button. Ordinarily this isn't necessary but could be useful in debugging.



Forcing An Expiry Run - This operation forces the Bayes software to take a look at the *token database* and determine if there are old tokens that are ready for removal. This is done on an automatic basis but can be done manually here by clicking on the *Proceed with Expiry* button in the *Bayes Database Maintenance* section of the web page. This could be useful when an admin wants to be sure that the database is up to date. A useful statistic to base such action is the *Time of Last Expiry Run*. If for some reason Bayes has not done an automatic expiry recently and the admin feels that the elapsed time is more than she likes she can do an expiry run manually. The configuration parameter that has a lot of influence on when this occurs on an automatic basis is the *Minimum Database Size* in the *General Configuration* web page under *Spam Configuration*. With a larger value the expiry runs will tend to be less often and with a smaller value they be more often. A larger database will provide more information for the system to make more accurate decisions but other administrative factors come in to play such as CPU, disk space, speed and available memory.

Clearing The Database Should it be necessary to clear the database use the *Proceed with Clear* button in the *Bayes Database Maintenance* section of the web page. This is a good idea before doing a database restore or when the admin wants to start building the database from a clean slate.

Backups and Restores This is vital in Bayes database maintenance. Over time a lot of valuable information will be stored in the Bayes database. Should the database become corrupted for some reason you don't want to start all over with seeding it and then having to wait the time it takes to accumulate the number of tokens that make up a mature system again. Create a new *Named Backup* for */home/vscan/.spamassassin* (this is where the database files live) and do daily full backups. Consult the EnGarde documentation on *System Backups* to get more details. If by chance your database gets

corrupted, clear the database described next and then do a normal restore from a recent full backup.

Summary

The following is a summary of the *Bayesian Filtering Subsystem*.

Database Maintenance Bayesian database has to be kept updated by teaching it spam and ham in fairly equal quantity.

Seeding the Database The *Bayesian Filter* will not run until it is taught with a minimum of 200 spam and 200 ham messages.

Learning Email Upload ham and spam in mbox format as described on page 66, to train the Bayesian database.

Forgetting Previously Learned Email The Bayesian Filter can forget incorrectly learned spam/ham. See page 66 for information about forgetting mail.

Auto Learning The Bayesian Filter can automatically learn from ham and spam passing through the spam filter, after the Bayesian database has been seeded. To enable this option, see page 59.

Rebuilding the Database You can rebuild the Bayesian database as described on page 69.

Forcing an Expiry Run You can expire old information in the Bayesian database, described on page 70.

Outbound Spam Protection

Outbound Spam Protection allows *Spam Scanning* to be disabled for certain domains. Doing this will allow all mail from the specified domain to be delivered without being scanned. This is mostly used for outbound mail which you would usually not want to be marked or rejected due to being determined as spam. You would list your top level, internal and subdomains here.

The general layout of the menu will show all existing domains on this whitelist. A domain may be listed with a '.' in front of it. This specifies that all of that domain's subdomains are also on this whitelist. For example, if *.guardiandigital.com* is listed in the *Outbound Domain Whitelist*, *new.guardiandigital.com* will also be exempt from spam scanning.

To edit an existing domain click on the associated *Edit* link found to the left of the domain. To add a domain click *New Outbound Whitelist Entry* found on the lower right portion of the menu. The following menu will appear.

Enter the domain name in the *Pattern* entry box. If every subdomain of this domain is to be on this whitelist check the *Adding a Whitelisted Domain* box. If this box is checked, two domain entries will appear on the menu after it is created, one for the domain and another for all of its subdomains. Click *Create Entry* to save and apply these changes.

NOTE: The domains specified for *Outbound Spam Protection* will also be the whitelist set of domains for protection from *Attachment Stripping*, found in *section 7.1.1* on page *47*.

Whitelists and Blacklists

Whitelists and *Blacklists* control which messages will be exempt from being scanned for spam and which messages will always be marked as spam on a sender and recipient basis, as opposed to a domain basis as in the *Outbound Spam Protection* section mentioned earlier.

Sender Whitelist
[Edit] sales@yahoo.com
[New Whitelist Entry]
Sender Blacklist
[Edit] spammer@domain.org
[Edit] *@spammers.org
[New Blacklist Entry]
Recipient Whitelist
[Edit] sales@guardiandigital.com
[New Recipient Whitelist Entry]
Spam Trap List
[Edit] trap@guardiandigital.com
[New Spam Trap List Entry]

Sender Whitelist These patterns define *From:* addresses that will be exempt from spam scanning. All messages from a sender address listed here will not be spam scanned.

Sender Blacklist These patterns define *From:* addresses that will always be tagged as spam.

Recipient Whitelist These patterns define *To:* addresses that will be exempt from spam scanning.

Spam Trap List These patterns define *To:* addresses that will always be tagged as spam. This is usually a *spam trap* email address set up to attract spam messages only. *Spam trap* email addresses are normally set up to create a database of spam messages (spam corpus), which can be used to teach Bayes manually.

Whitelisting mailing lists requires entries in both the *Sender Whitelist* and the *Recipient Whitelist* in order to work correctly. You can create an entry simultaneously in both of these access lists by clicking the *Clicking Here* link.

For specifying domains, use **domain.com.* This pattern will match the subdomains also. For just the domain, use **@domain.com*. For particular users, use *user@domain.com*

Note: Remember that the whitelisting and blacklisting is based on information in the e-mail header, which can be easily forged. For example, If a spam sender

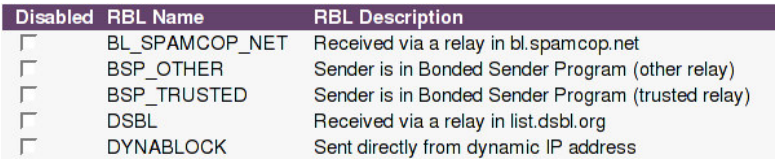
gains knowledge of a whitelisted sender address, he can forge the *From:* field in the header and send mail bypassing spam scanning. It is recommended that contents of the whitelists be considered sensitive.

RBL Settings

The *RBL Setup* menu allows configuration of the RBL (Real-time Black-hole Lists) to be used with this server. The first option is to *Enable* or *Disable* this server to use this functionality.

RBL checks must be *Enabled* for any of the following options to work. Also, remember that *Remote Tests* must be enabled in *CAPE Center::Mail Filters::General Filter Settings::Filter Configuration* for RBLs to work.

RBLs are a free service. These RBLs contain lists of hosts known to send spam. The spam filter contacts the RBL servers located on the Internet and if the message sender is listed in an RBL, a particular number of points is added to the total spam score of the message. You can enable or disable different RBL checks. All RBLs are enabled by default. To disable a RBL, check the corresponding box to the left.



Disabled	RBL Name	RBL Description
☐	BL_SPAMCOP_NET	Received via a relay in bl.spamcop.net
☐	BSP_OTHER	Sender is in Bonded Sender Program (other relay)
☐	BSP_TRUSTED	Sender is in Bonded Sender Program (trusted relay)
☐	DSBL	Received via a relay in list.dsbl.org
☐	DYNABLOCK	Sent directly from dynamic IP address

7.1.5 Virus Configuration

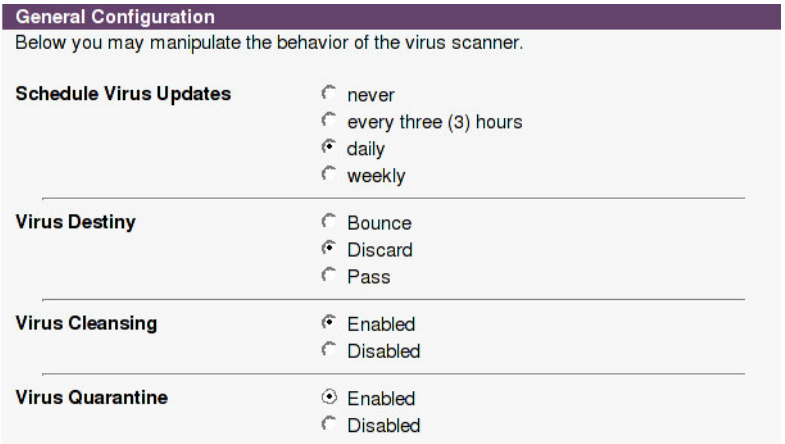
The *Secure Mail Suite* has the capability to scan all incoming and outgoing e-mail attachments for known viruses. The *Virus Configuration* menu allows control over this functionality through the following menu.

You can view the engine version and the time the virus rules were last updated on the top of the page. The engine should be kept updated using the GDSN. You can schedule virus updates using the options below. To update the rules immediately, click *Update Rules.*

General Configuration

Here you can adjust the behavior of the virus scanning subsystem and specify how often to update the virus rules. Remember that *Virus Scanning* should be enabled in *CAPE Center::Mail Filters::General Filter Settings::Filter Configuration* before editing the options here.

NOTE: You must update the virus data at least once before virus scanning will work. Do this by clicking on *Update Rules* which requires a virus update license.



Schedule Virus Updates How often to update the virus rules. It is very important that virus rules are kept updated. It is recommended that you set this to daily. At time of new virus outbreaks, you may want to update virus rules every three hours.

Virus Destiny Here you can specify the fate of a message that contains virus. The following options are available:

- *Bounce* The message is not delivered, and is bounced back to the sender.
- *Discard* The message is not delivered and is not bounced back to the sender. In this case, the server will acknowledge receipt of the mail, but will discard it silently. This is the recommended option.
- *Pass* The virus will be delivered to the recipient. Never set this option to *Pass.*

Virus Cleansing If this option is *Enabled,* a virus found in an attachment will be cleansed, and the e-mail will go through, if possible. If this is *Disabled* then the e-mail will be subject to the *Virus Destiny*.

> **NOTE:** If an e-mail carries a digital signature, cleansing a virus from that e-mail will alter the original e-mail which will break the digital signature.

Viruses Quarantine Enabling *Quarantine Viruses* will quarantine all infected emails. This will be done regardless of how *Virus Destiny* is set. Quarantined messages can be viewed in the *Message Quarantine* section of the *CAPE Center*.

Virus Notification

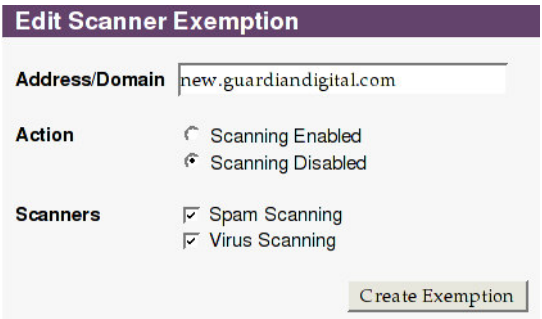
When an infected attachment is found, a report is made stating that the e-mail had a virus, an attempt to cleanse it was made, and the results of the cleansing, if cleansing is enabled. You can specify here who should receive these reports. If *Message Sender* is checked, the notification will be sent to the message sender. This action is strongly discouraged due to the high volume of viruses with faked sender addresses. If *Message Recipient* is checked, the notification will be sent to the recipient. If *Administrator* is checked, then the notification email will be sent to the *virus-admin* alias (which by default goes to the *admin* user) every time a virus is found. If you checked *Virus Admin* option, you must make sure that the alias *virus-admin* exists, and points to a real email address. This can be done in the *Aliases and Routing* section.

After editing the settings, click on the *Save Settings* button to save the new configuration.

7.1.6 Spam/Virus Scanner Exemptions

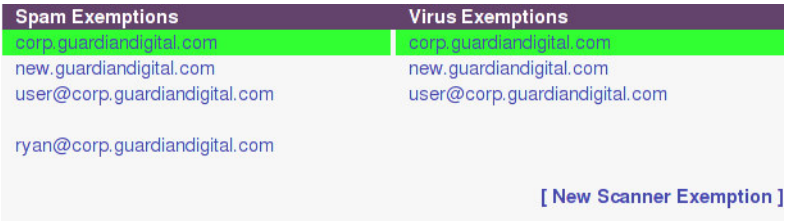
All virtual domains and mail routes defined on this server are scanned for viruses and spam by default when virus and spam options are enabled. In this section, you can exclude certain users and domains from spam/virus scanning. If a domain in listed in the *Scanner Exemptions,* mails addressed to that domain will not get scanned.

To create an exemption, click on the *New Scanner Exemption* button. A popup window will appear. Enter the email address or the domain name on the *Address/Domain* field. The *Action* specifies whether scanning will be enabled or disabled for this address/domain. The *Scanners* option can be used to define whether the action is taken for virus scanning, spam scanning or for both. For example, if the *Action* is set to *Scanning Disabled* and only *Virus Scanning* is checked in the *Scanners*, then mail to the corresponding domain will not be scanned for viruses, but will be scanned for spam.



All exemptions are listed on this page. Exemptions for email addresses take precedence over domains. So you may disable scanning for a domain, but enable scanning for certain email addresses in that domain, and vice versa. Addresses and domains listed in the green background gets scanned, and others are exempted from scanning.

In the screenshot example below, all mail to addresses in the domain *corp.guardiandigital.com* gets scanned, but mail to the email address *user@corp.guardiandigital.com* will not be scanned. You may edit an exemption by clicking on the domain name.



7.2 SMTP Access Controls

The *Access Controls* section allows for very fine-grained tuning of access to the server. Access to the server can be denied or granted based on the recipient address, sender address and the IP address or hostname of the *SMTP Client.*

The main menu has two main options on it. *Enable Recipient Address Controls* and *Enable Sender Address Access Controls*. Below the buttons are the sections for configuring both these options, which are inaccessible until they are enabled. *SMTP Client Access* is always enabled.

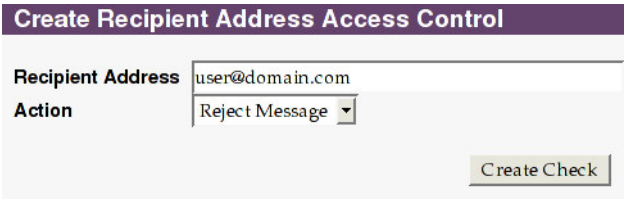
You need to enable *Recipient Address Access Control* and *Sender Address Access Control* before using them.

7.2.1 Recipient Address Access Controls

Here you can control access to the server based on the recipient address in the mail. The server can deny relay access based on the recipient address in the mail.

All *Recipient Address Access Controls* are listed in this section. In the example, all mail to the email address *user@domain.com* will be denied access to the server.

To create a new *Recipient Address Access Control*, click *New Recipient Address Access Control.*



Recipient Address The recipient address to be blocked. Acceptable sender definitions are in the format *user@domain.com, @domain.com* and *user@*.

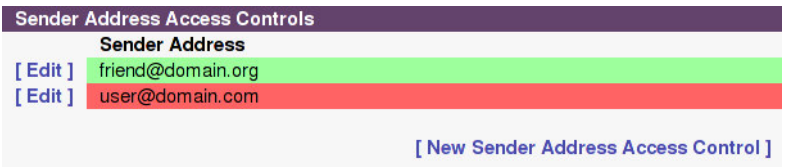
- *user@domain* Blocks the address *user@domain* only.
- *@domain* Blocks all recipients in the domain *domain.com.*
- *user@* Blocks all recipients with the name *user.*

Action Action to be taken by for mail matching the recipient address above. The only option is to reject the message.

To edit a *Recipient Address Access Control*, click *Edit.*

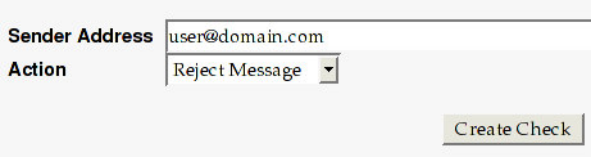
7.2.2 Sender Address Access Controls

The *Sender Address Access Controls* is based on the envelope sender address of the mail, which most of the time matches the *From:* field, but not always.



The interface works similar to the *Recipient Access Controls* described above. Its priority is higher than that of *Recipient Address Access Control*. In the example, a mail with *From:* address *user@domain.com* will be denied access. Sender addresses marked in red are denied access, while those marked green are allowed.

To create a new *Sender Address Access Control* rule click the *New Sender Address Access Control* link.



Sender Address Acceptable sender definitions are *user@domain.com*, *domain.com* and *user@*. *"user@"* matches all senders with name *user*.

Action The pull-down menu has the option to *Reject Message* or *Accept Message*.

Once the fields have been filled in, click *Create Check* and the new rule will appear on the main screen below *Sender Address Access Controls*.

NOTE: Applying the *Accept Message* action to a sender address gives relay access to an external user based on the *From:* mail header. Any external user that has knowledge of these sender addresses can easily forge this header, and gain relay access to this mail server. It is highly suggested you use pop-before-smtp before resorting to this service to permit relay access. If using this service is the only available option, then realize that the data entered here needs to be considered sensitive.

7.2.3 SMTP Client Access Controls

The SMTP Client Access Controls define which servers are allowed to connect to the mail services to send mail using SMTP.

SMTP Client Access Controls
Client
[Edit] machine1.corp.guardiandigital.com
[Edit] corp.guardiandigital.com
[Edit] 192.168.3.34
[New SMTP Client Access Control]

The rules are applied in the order shown top to bottom, the top being the first and the bottom being the last. Once a rule matches a client, the associated action is taken and the rule matching is stopped. When you create a new rule it will automatically be listed in the order that the mail system applies them. You cannot change this order. Acceptable client definitions are *domain.com*, *full IP address* (xxx.xxx.xxx.xxx), or *network IP address* (xxx.xxx.xxx.). Using the example from the screen-shot above, *corp.guardiandigital.com* was given access to use the mail server. However, two machines were blocked out, *machine1.corp.guardiandigital.com* and 192.168.3.34.

To add a new *SMTP Client Access Control* click the *New SMTP Client Access Control link*. A new window will appear labeled, *Create SMTP Client Access Control*.

Client This is the client machine or network that will be the focus of this access control item.

Actions This is a pull-down menu that determines if this access control item will be used to accept the message the reject it.

Once the fields have been filled, click *Create Check* and the new rule will appear on the main screen below *SMTP Client Access Controls*.

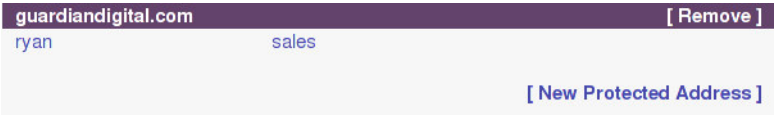
To edit or delete an access control entry, click the *Edit* link. This will bring up a new window with the option to edit or delete the access control entry.

NOTE: Access control based on *SMTP Client* has a higher priority than that of the *Recipient Address*, but lower than that of *Sender Address*.

7.3 Recipient Policy

You can define exclusive recipient lists (local, aliased, or relayed) on a domain/ hostname basis. You may create a protected domain and define a number of mail addresses in that domain. Only the specified addresses in the protected domain will be allowed access. This feature provided effective protection against spam mail that is sent to non-existent addresses in a domain.

In the example, suppose the relay server *corp.guardiandigital.com* relays mail for the domain *guardiandigital.com* to the machine *mailbox.guardiandigital.com*. Suppose the email address *user@guardiandigital.com* doesn't exist. Normally, a mail sent to that address will be relayed by *corp.guardiandigital.com* to *mailbox.guardiandigital.com* where it will be bounced. By defining *guardiandigital.com* as a protected domain on the relay server *corp.guardiandigital.com,* we can reject the mail from the relay server itself, instead of having to be forwarded to mailbox.guardiandigital.com first. For this, we need to define all valid addresses existing in the domain *guardiandigital.com* in the relay server. When the relay server receives a mail for *guardiandigital.com*, it checks the recipient name in the database and will relay it to *mailbox.guardiandigital.com* only if it is listed there.



Most spam email are addressed to non-existent addresses and by protecting a domain we can save a lot of non-necessary traffic and resource usage. Make sure that if a domain is protected, all addresses existing in the domain are listed under that domain. Mail to addresses in a protected domain not listed here will be denied access as if the user does not exist here.

You can protect all, some, or none of your domains in this manner. Please remember that once a domain is protected, all addresses in the domain must be listed here. This server will allow only the addresses listed here in this domain.

To enable *Recipient Protection*, select *Enabled* and click *Save.* The recipient protection will be effective only if it is enabled here.

7.3.1 Creating a New Protected Domain

To create a protected domain, enter the domain name or hostname in the *New Protected Domain/Host* field and click *Save.* When a domain is created, it will be listed on the bottom of *Recipient Policy* page.

7.3.2 Adding Protected Addresses

When a protected domain is created, you must list all addresses in that domain here. To create a new *Protected Address* in the protected domain/host, click *New Protected Address*. A pop-up window will be displayed where you can enter the address. Click *Create Address* to add the address to the protected domain. When an address is added to a protected domain it will be listed below the domain. You can edit an address by clicking on the name.

Removing A Protected Domain To remove a domain, click on *Remove* link to the right of the domain.

7.4 Spam/Virus Quarantine

If *Spam/Virus Quarantine* is enabled, messages detected as spam or virus will be stored in the quarantine database. In the *Spam/Virus Quarantine* section, the administrator can view quarantined spam and virus messages. Quarantined messages can optionally be forwarded to the recipient by the administrator. Usually, on servers handling heavy mail traffic, the quarantine database can become quite large. A search facility is provided, which is quite useful for managing large quarantine databases.

You can search the quarantine database based on the received date, mail headers *(From:, To*: and *Subject:*), and message size. Number of messages in both spam and virus quarantines will be shown on the top of the page

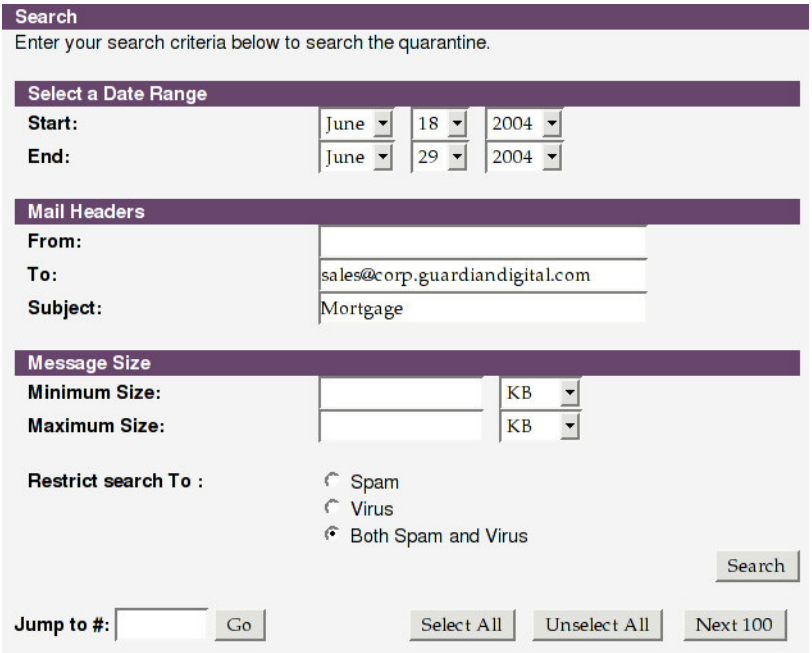
There are **5** messages in the spam quarantine.
There are **26** messages in the virus quarantine.

7.4.1 Search Criteria

Date Range You may select a start date and an end date. The search results contain only those mails received between the two dates.

Mail Headers You can search using the *Sender Address* (*From:*), *Recipient Address* (*To:*) and the *Message Subject*. The search result will contain only those messages having the patterns in the corresponding headers. For example, searching for *@corp.guardiandigital.com* in the *To:* field will show mails addressed to any user in the domain *corp.guardiandigital.com.*

Message Size You can specify minimum and maximum size of messages. The search result will contains messages in the specified size range only.

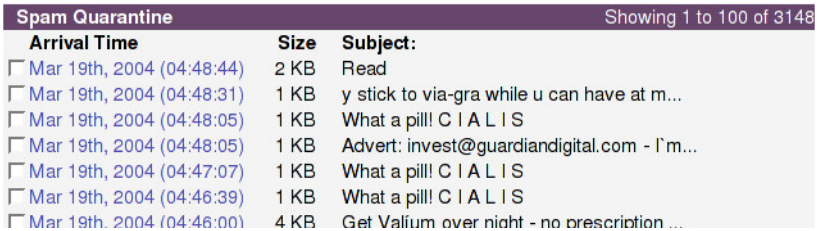


If a field is empty, that particular criteria will not be used in the search. You may restrict search to spam quarantine or virus quarantine, or search both at a time.

The search result will list first 100 results in both categories. If there are a lot of messages in the *spam quarantine,* you will need to scroll down to see the *virus quarantine.* You can jump to any part of the quarantine by entering the message number in the *Jump To*: field and clicking *Go*.

7.4.2 Viewing Messages

The menu is broken down into two sections, *Spam Quarantine* and *Virus Quarantine*.


Spam Quarantine
Showing 1 to 100 of 3148
Arrival Time
Size
Subject:
Mar 19th, 2004 (04:48:44) 2 KB Read
Mar 19th, 2004 (04:48:31) 1 KB y stick to via-gra while u can have at m...
Mar 19th, 2004 (04:48:05) 1 KB What a pill! C I A L I S
Mar 19th, 2004 (04:48:05) 1 KB Advert: invest@guardiandigital.com - I`m...
Mar 19th, 2004 (04:47:07) 1 KB What a pill! C I A L I S
Mar 19th, 2004 (04:46:39) 1 KB What a pill! C I A L I S
Mar 19th, 2004 (04:46:00) 4 KB Get Valium over night - no prescription ...

By clicking on the date associated with the spam/virus to be viewed, a window will appear with more detailed information concerning the item. From this new window the detailed item will appear. There will be an option at the top to forward the e-mail to a specified recipient (only for spam). If this is chosen a new window will appear with an entry box for the e-mail address the e-mail will be sent to.

7.4.3 Deleting Messages from Quarantine.

To delete a message from the quarantine, click on the corresponding checkbox, and click *Delete Selected Messages* on the bottom of the screen. You can select/unselect all displayed messages using the buttons *Select All* and *Unselect All.*

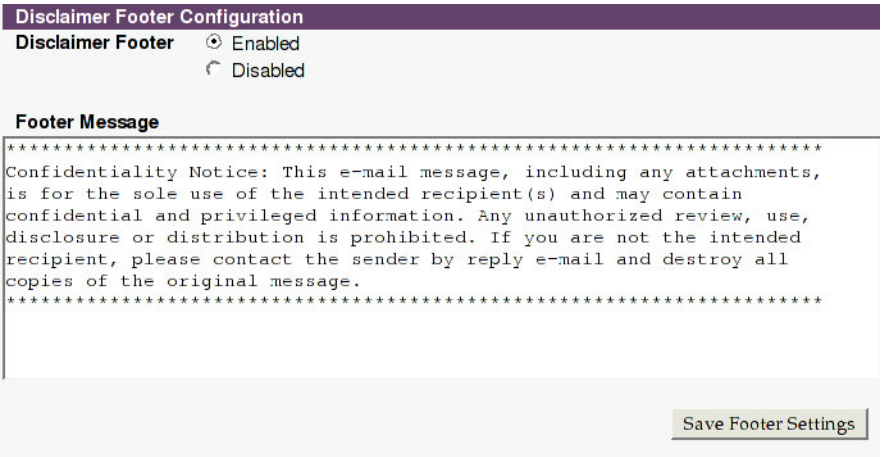
7.5 Disclaimer Footer

The *Disclaimer Footer* allows an e-mail footer, to be appended to all outgoing e-mail from the server.

A *Disclaimer Footer* can simply be a brief corporate policy statement or something like a company slogan.

Disclaimer Footer If *Disclaimer Footer* is set to enabled, the content of the *Footer Message* will be appended to each outgoing e-mail. If disabled it will not be appended but text in the *Footer Message* will still remain saved in the system.

Footer Message The message to be displayed at the bottom of each outgoing e-mail can be entered into this entry box. Each line in the message should not exceed 74 characters in length.


Disclaimer Footer Configuration
Disclaimer Footer
Enabled
Disabled
Footer Message
****
Confidentiality Notice: This e-mail message, including any attachments,
is for the sole use of the intended recipient(s) and may contain
confidential and privileged information. Any unauthorized review, use,
disclosure or distribution is prohibited. If you are not the intended
recipient, please contact the sender by reply e-mail and destroy all
copies of the original message.
****
Save Footer Settings

Once changes have been made click the *Save Footer Settings* to make the changes.

8 Configuring the LDAP Database

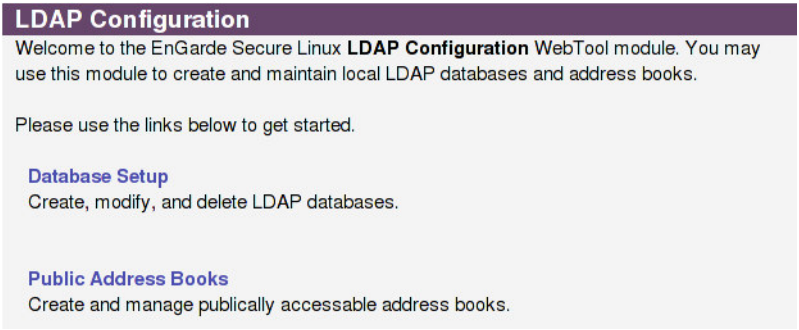
The Guardian Digital WebTool implements an LDAP server. This can be found in the *System Management* menu under the *Service Configuration* section. The included LDAP server is used for address books and by the mail server itself to maintain aliases and virtual domains.

During installation there is the option to install the LDAP database. If it was installed it must first be configured and the database initialized before it can be used by the mail server.

NOTE: The LDAP database capability is only available with the Corporate and Enterprise versions of Secure Mail Suite.

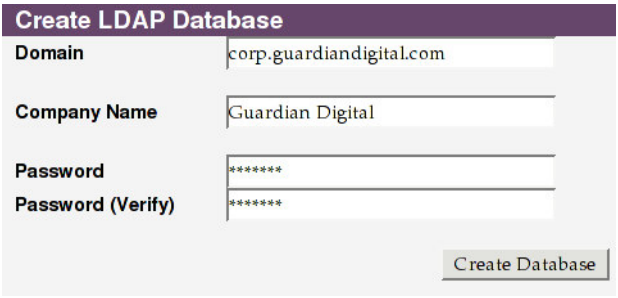
8.1 LDAP Configuration

To start configuration of the LDAP server log in to the WebTool and select *System Management*. In the *System Management* menu under *Service Configuration* there will be a new option, *LDAP Configuration*; Select it.


LDAP Configuration
Welcome to the EnGarde Secure Linux LDAP Configuration WebTool module. You may use this module to create and maintain local LDAP databases and address books.
Please use the links below to get started.
Database Setup
Create, modify, and delete LDAP databases.
Public Address Books
Create and manage publically accessable address books.

The *LDAP Database* menu will be empty prior to any databases being created. A new database must be created at this point. Click *Create Database*.

A new window will open containing the *Create LDAP Database* menu. Each field must be completed for the database to be created.

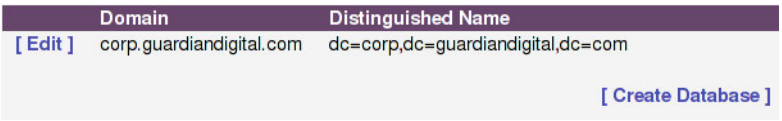


Domain The *Domain* for this database should be the domain the server is located on. This domain will be used for the LDAP database's *Distinguished Name*. For example, if *corp.guardiandigital.com* is entered in as the *Domain* then the *Distinguished Name* (DN) would be *dc=corp,dc=guardiandigital,dc=com*.

Company Name The *Company Name* should be the name of the company that this database will be associated with. This *Company Name* will be stored in the main database entry when the database is created.

Password This is the password that will be required when the LDAP database needs to be bound to for full access. A strong password is recommended for this.

Once all of these fields have been completed, click *Create Database*. It will take a few moments for the database to be created. Once it has been completed the database will appear in the *LDAP Database* menu.



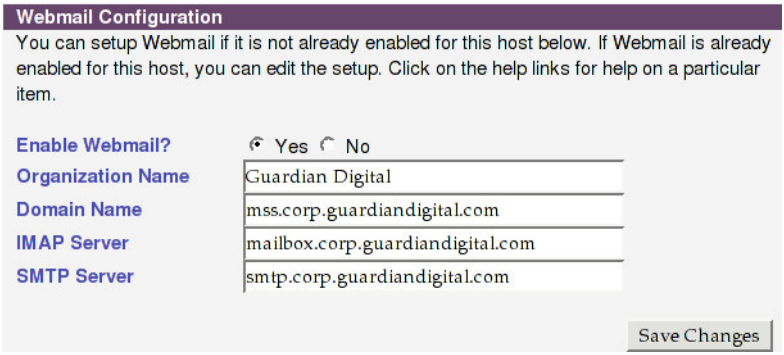
You can edit a database by clicking the *Edit* link located to the left of the respective database. When clicked a new window will appear containing the *Edit LDAP Database* properties. This menu resembles the *Create LDAP Database* menu with the added ability to delete the database.

9 Configuring Webmail

Webmail is a Web based interface that allows a user to send and receive their e-mail via the web in their browser. *Webmail* will connect to your mail server via an IMAP connection for receiving and SMTP connection for sending mail. It will format messages into HTML for the user to view and respond to in their browser.

Webmail works from an SSL virtual host, so a SSL virtual host must be present prior to enabling *Webmail.* For information regarding creation of an SSL virtual host refer to *section 4.3.1* on *page 56* of the EnGarde User Manual.

The *Webmail* configuration can be found when editing a *Secure Virtual Host* by selecting the *Webmail Configuration* option. Webmail can be enabled and configured through that menu.


Webmail Configuration
You can setup Webmail if it is not already enabled for this host below. If Webmail is already enabled for this host, you can edit the setup. Click on the help links for help on a particular item.
Enable Webmail?
Yes
No
Organization Name
Guardian Digital
Domain Name
mss.corp.guardiandigital.com
IMAP Server
mailbox.corp.guardiandigital.com
SMTP Server
smtp.corp.guardiandigital.com
Save Changes

Enable Webmail Selecting *Yes* here will enable Webmail for the specified virtual host. If this is already set to *Yes,* then by setting it to *No* you will remove the existing *Webmail* services, including the configuration files and profiles.

Organization Name This organization name will show up on several Webmail screens.

Domain Name This is the domain name that all outgoing e-mail will be from.

IMAP Server This is the IMAP server that the Webmail system should connect to. This should be kept as the default *localhost* unless you want to connect to an external IMAP server.

SMTP Server This is the SMTP server that all outgoing webmail will go to. This should be kept as the default *localhost* unless you want to relay email through an external mail server.

When all changes are done, click the *Save Changes* button to save and apply these changes. You must also restart the web server. This can be done in the *Virtual Host Management* page.

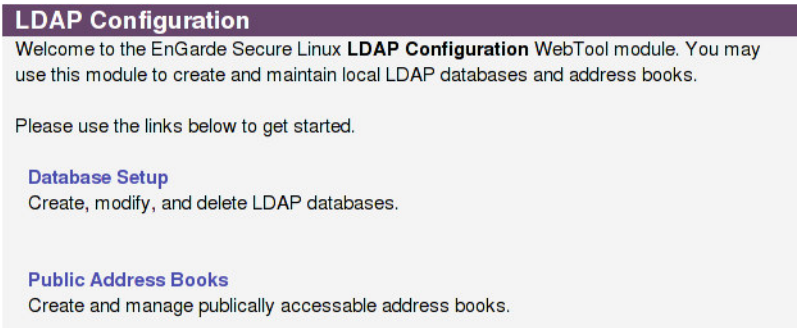
10 Public Address Books

With the LDAP server installed and a database created (see *Section 8* on page *87* regarding this) public address books can now be created.

An address book is a set of names, phone numbers and e-mail addresses for a group of people. By entering this information into an LDAP server it becomes readily available to users on the network, keeps the data consistent across the network and is fully compatible with all major e-mail clients.

10.1 Create a New Address Book

To create a new address book select *LDAP Configuration* from the *System Management* menu in the WebTool.

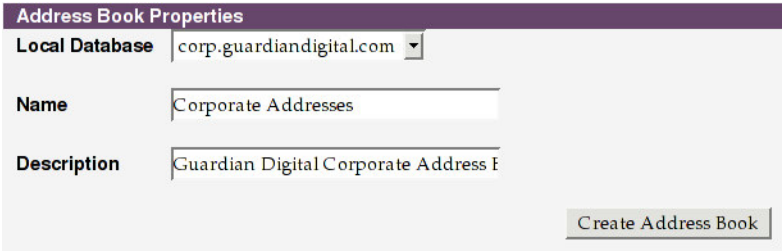

LDAP Configuration
Welcome to the EnGarde Secure Linux LDAP Configuration WebTool module. You may use this module to create and maintain local LDAP databases and address books.
Please use the links below to get started.
Database Setup
Create, modify, and delete LDAP databases.
Public Address Books
Create and manage publically accessable address books.

The *LDAP Database* menu will appear. Click the *Public Address Books* options.

The *Public Address Books* menu will appear. On this menu will be a list of all the address books in the databases. There will be none listed if no address book have been created.

To create a new address book click *Create Public Address Book*.

A new window will appear with all the options for a new address book. Each item must be completed before the address book can be created.



Local Database From the pull-down menu choose the database that will host this address book.

Name The name of the address book. This name will be used when configuring the client-side as well.

Description This is a more detailed description of what the address book contains. This description will appear if someone does a search of all accessible address books.

Once all the fields have been completed click the *Create Address Book* button. The address book will be created and now listed in the menu.

To edit or delete the address book click the *Edit* link found to the left of the respective address book. A menu similar to the *Create Public Address Book* window will appear. Here options are provided for deleting, making changes or creating address book entries.

NOTE: When an address book is deleted ***all*** entries within the address book are deleted as well.

The new address book will be accessed by its *Distinguished Name (DN)*. This *DN* is determined by the *Domain* that was selected when the database was created that the address book is configured to use and by the *Name* of the database.

Using the previous example, the *Domain* that the database is configured for uses *corp.guardiandigital.com* and the *Name* assigned to the example address book is *Guardian Digital Corporate Address Book*. Therefore this address book would be accessible through the *Distinguished Name* of:

cn=Guardian Digital Corporate Address Book,cn=address_books, ou=public_services,dc=corp,dc=guardiandigital,dc=com.

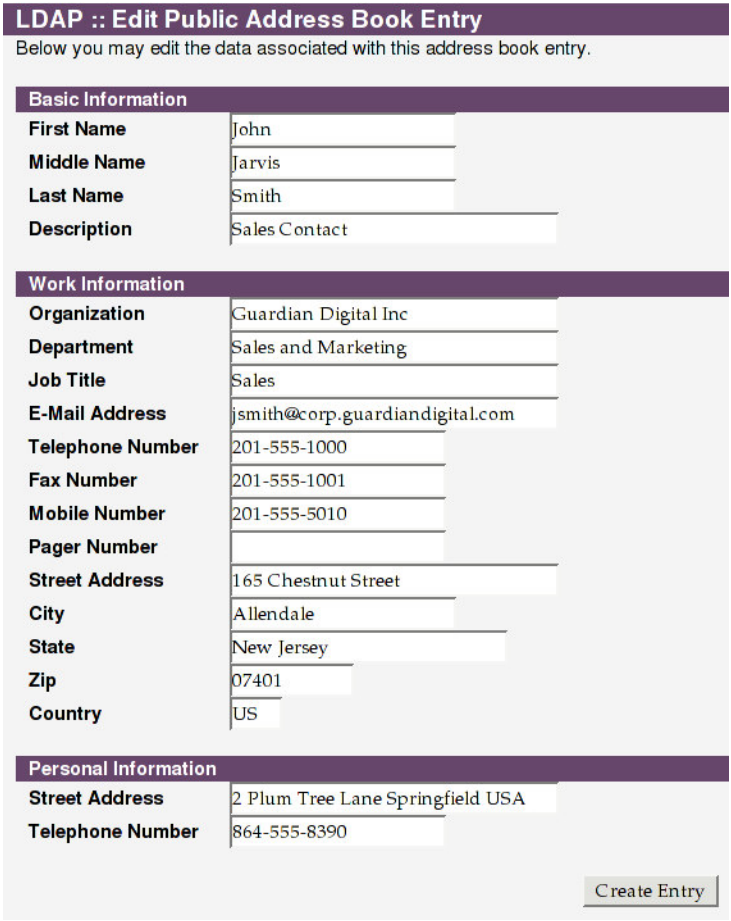
10.2 Create a New Address Book Entry

An address book needs to have entries in it to be of any use. To create an address book entry go to the *Public Address Books* menu found in the *LDAP Configuration* menu in the *System Management* menu.

In the *Public Address Books* menu will be a list of all address books. If none exist, create a new one. Refer to section *10.1* on page *91* for doing this. Next to each address book an *Edit* link can be found. Click the *Edit* link corresponding to the address book that the entries will be created in.

Located after the *Address Book Properties* will be the *Address Book Entries* section. Each entry will be listed in this section. To create a new entry click the *New Entry* option.

A new window will appear with all the necessary fields for creating a new address book entry. The only required fields are *First Name*, *Last Name*, *E-Mail Address* and *Country*.



Once all the necessary fields have been appropriately filled in click the *Create Entry* button to enter this entry into the LDAP database. Once it has been added it will be listed under the *Address Book Entries* portion of the menu.

To edit or delete an entry click on the *Edit* link found to the left of the corresponding entry. A new window will open, similar to creating a new entry with the additional option to delete or update the entry.

11 Secure User Manager

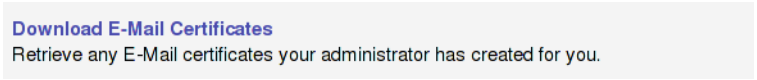
EnGarde Secure Linux provides a end-user control panel to control basic administration tasks such as password maintenance and secure shell (SSH) key maintenance.

With *Secure Mail Suite* the users now have the ability to download their e-mail certificates, set up forwarding addresses, manage their vacation messages and adjust their own spam filtering settings.

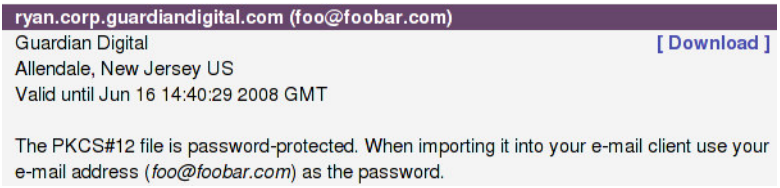
For more information regarding the *EnGarde Secure User Manager* refer to *Section 4.8* on page *169* of the *EnGarde User Manual.*

11.1 Downloading User E-Mail Certificates

Once logged into the *EnGarde Secure Manager,* the e-mail certificate(s) can be found by clicking on *Download E-Mail Certificates*.



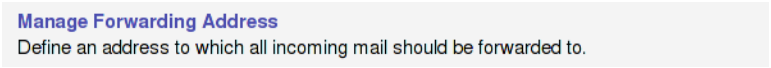
The *Download E-Mail Certificates* menu will be displayed with each certificate listed. Following the certificate is a link, *Download*. Click the link to download and save the certificate to the local system.


ryan.corp.guardiandigital.com (foo@foobar.com)
Guardian Digital
[Download]
Allendale, New Jersey US
Valid until Jun 16 14:40:29 2008 GMT
The PKCS#12 file is password-protected. When importing it into your e-mail client use your e-mail address (foo@foobar.com) as the password.

11.2 Manage Forwarding Address

The user can optionally forward all the mail delivered to his email address to another email address. In this section, the user can provide a forwarding address and setup email forwarding.

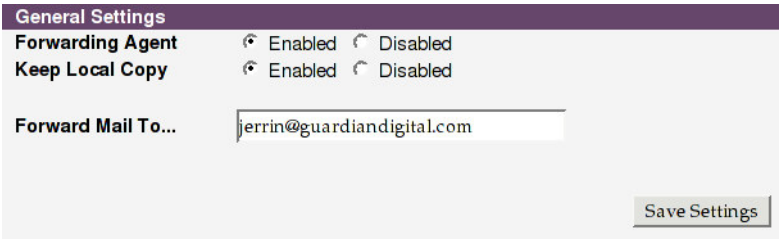
Remember that the user can access this section only if he is allowed in *Secure User Manager* (section 6.1.2, page 16).



Manage Forwarding Message can be accessed by clicking on *Manage Forwarding Message* from the main screen of *Secure User Manager*.

11.2.1 General Settings

The *General Settings* section allows you to setup the forwarding address.



Forwarding Agent You can enable or disable email forwarding here. If enabled, all email to this user will be forwarded to the email address provided below. The following options will be valid only if you enable this option.

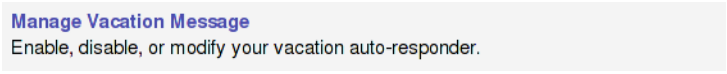
Keep Local Copy In addition to forwarding the email, deliver it to the local address also. If enabled, the user will receive a copy of all email addressed to him and they will be forwarded to the forwarding address also. If disabled, the mail will not be delivered to the user's local mailbox.

Forward Mail To The email address for forwarding the mail to. All mail the user receives will be sent to this email address.

11.3 Managing the Vacation Message

When a user is out of the office and/or does not have access to their e-mail for an extended period of time, an auto-responding message can be configured. This message will be sent out in reply to all incoming e-mail.

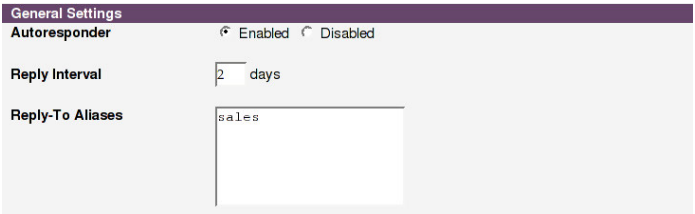
Remember that the user can access this section only if he is allowed in *Secure User Manager* (section 6.1.2, page 16).



Manage Vacation Message can be accessed by clicking on *Manage Vacation Message* from the main screen of the *Secure User Manager*.

11.3.1 General Settings

The *General Settings* section has the following options for configuring the *Vacation Message.*



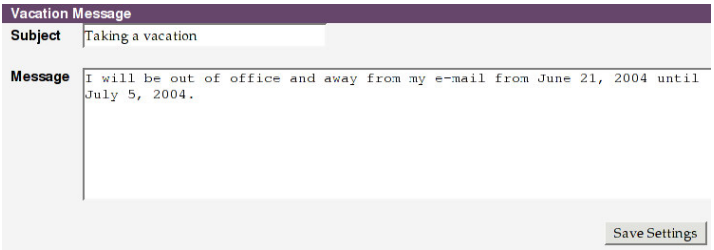
Auto-responder The options in the *Auto-responder* are to *Enable* or *Disable*. If disabled then no vacation message will be sent out regardless of any settings made following this.

Reply Interval This *Reply Interval* sets the number of days each auto-reply should be sent. For example, if set for two days then a person who sends the user and e-mail will get the vacation message in response. Then if the user sends a few more messages within a two day period no additional vacation responses will be sent until a message is sent after the two day period.

Reply-To Aliases The *Reply-To Alias* allows multiple aliases associated with the user's e-mail address to be specified. By default if an e-mail is sent to a user's alias the auto-responder will not reply to it unless it's listed here.

11.3.2 Vacation Message

The *Vacation Message* section allows the actual message to be configured. Both the body of the message and the subject can be configured here.


Vacation Message
Subject
Taking a vacation
Message
I will be out of office and away from my e-mail from June 21, 2004 until July 5, 2004.
Save Settings

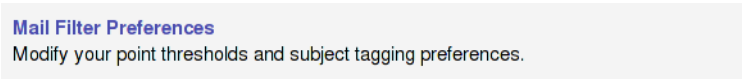
Subject The *Subject* is the line that will appear as the subject of the message.

Message This *Message* is the body of the e-mail.

11.4 Mail Filter Preferences

In this section, users can set up their own spam filter settings. Users can change the spam score thresholds which determine the sensitivity of the spam filter for messages addressed to them. Users can set up their own whitelist and blacklists for spam filtering and they can disable/enable spam tagging. The user can access this section only if he is permitted by the administrator in the *Secure User Manager* section (section 6.1.2 on page 19) and *User Preferences* is enabled in section 7.1 on page 44

To access this section, click *Mail Filter Preferences*.



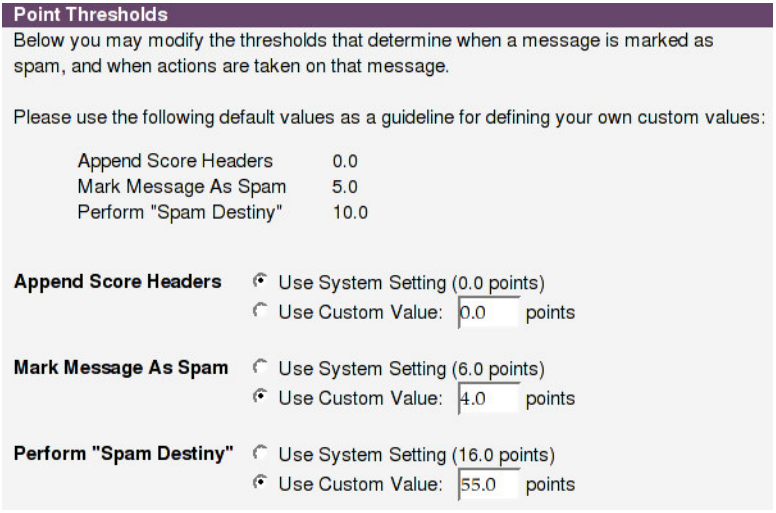
This section has the following parts:

11.4.1 Point Thresholds

When the mail filter scans a mail for spam, it calculates a spam score. This score is a direct measure of the likelihood that the mail is spam. A message which results in a higher spam score is more likely to be a spam than a message with a lower score. The spam filter takes into account a wide array of techniques in the calculation of this score, which includes Bayesian analysis and network tests.

A mail having absolutely no characteristics of spam gets a score of 0. Generally, if the score of a mail is greater than 5, we can say with a resonable amount of confidence that the mail is spam.

Secure Mail Suite allows the administrator to set thresholds for mail to be considered spam. These thresholds apply for all users. However, the users can use this section to set their own spam score thresholds which apply only to mail addressed to them. If the score of the mail is greater than the specified threshold, the corresponding action will be taken for the mail.


Point Thresholds
Below you may modify the thresholds that determine when a message is marked as spam, and when actions are taken on that message.
Please use the following default values as a guideline for defining your own custom values:
Append Score Headers 0.0
Mark Message As Spam 5.0
Perform "Spam Destiny" 10.0
Append Score Headers
Use System Setting (0.0 points)
Use Custom Value: 0.0 points
Mark Message As Spam
Use System Setting (6.0 points)
Use Custom Value: 4.0 points
Perform "Spam Destiny"
Use System Setting (16.0 points)
Use Custom Value: 55.0 points

The thresholds are described as follows:

Append Score Headers This is the threshold for determining whether to append spam score information to the header of each mail. The score header contains detailed information about the spam tests triggered by this mail, and the score each of them contributed to the total spam score of this mail. This

information is helpful when debugging the spam filter or to determine why a mail was classified incorrectly.

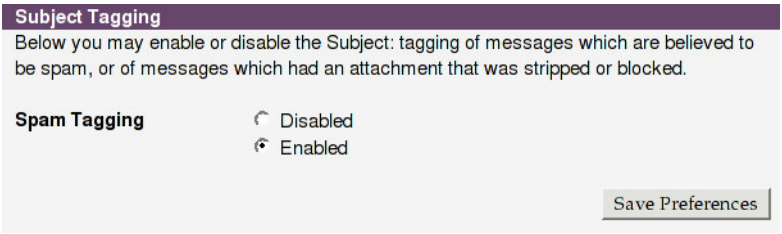
Mark Message As Spam If this threshold is exceeded, the subject of the message will be tagged. The subject tag is specified by the administrator. Recommended value for this threshold is 5.0.

Perform Spam Destiny If this threshold is exceeded, the mail will be subjected to the *Spam Destiny*. The *Spam Destiny* can be *Bounce* (bounce the message back to the sender; don't deliver it to the recipient), *Discard* (don't deliver or bounce the message) or *Pass* (deliver it to the recipient) and is set by the administrator.

For each of these thresholds, you can either use the system setting (value set by the administrator) or use custom setting (your own threshold).

11.4.2 Subject Tagging

The user can enable or disable subject tagging. If enabled, the subject tagging will be performed for mail believed to be spam or had attachments stripped or blocked. If disabled, mail for this user will not be tagged.


Subject Tagging
Below you may enable or disable the Subject: tagging of messages which are believed to be spam, or of messages which had an attachment that was stripped or blocked.
Spam Tagging
Disabled
Enabled
Save Preferences

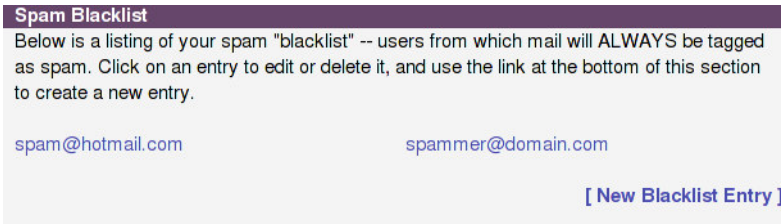
11.4.3 Spam Whitelist

Spam whitelist contains email addresses from which mail will never be tagged as spam. To create a whitelist entry, click *New Whitelist Entry.* Enter the pattern in the pop-up window and click *Create Entry*. Existing whitelist entries will be listed in this section. To edit or delete an entry, click on it and use the controls in the pop-up window.

Spam Whitelist
Below is a listing of your spam "whitelist" -- users from which mail will never be tagged as spam. Click on an entry to edit or delete it, and use the link at the bottom of this section to create a new entry.
news@guardiandigital.com
sales@guardiandigital.com
user@domain.com
[New Whitelist Entry]

11.4.4 Spam Blacklist

This is the blacklist of email addresses which will always be tagged as spam. To create a blacklist entry, click *New Blacklist Entry*. Enter the pattern in the pop-up window, and click *Create Entry*. Existing blacklist entries will be listed in this section. To edit or delete an entry, click on it, and use the controls in the pop-up window.


Spam Blacklist
Below is a listing of your spam "blacklist" -- users from which mail will ALWAYS be tagged as spam. Click on an entry to edit or delete it, and use the link at the bottom of this section to create a new entry.
spam@hotmail.com
spammer@domain.com
[New Blacklist Entry]

11.5 Spam/Virus Quarantine

This section allows local users to view their quarantined messages. If virus and spam quarantine is enabled, then suspected mail will be quarantined in a local database. A local user can view quarantined mail for which he was either the recipient or the sender. The user can forward or delete a quarantined mail. They can search the quarantine database using the mail sender, recipient, message subject, message size and the date of the message.

To access this section, click *Spam/Virus Quarantine*. Managing this section is quite similar to the general *Spam/Virus Quarantine* section, outlined in section

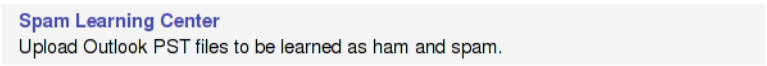
7.4, on page 83, except that this section will display only those mail sent by, or addressed to, the local user. You may refer to that section for detailed information about searching the quarantine or forwarding and deleting quarantined mail.

11.6 Spam Learning Center

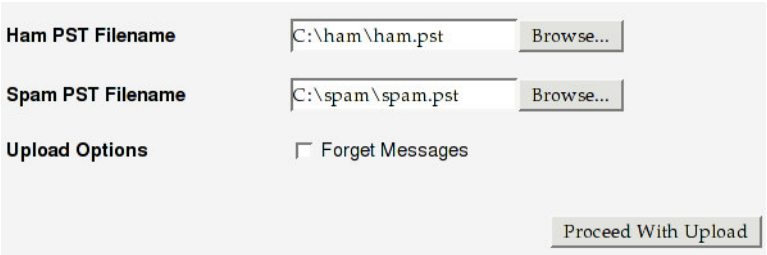
This section allows the local users to train the Bayesian spam filtering database by uploading their spam and ham email. You can upload the PST (Personal File Folder) files exported from Microsoft Exchange. Refer section *Exporting PST's From Outlook (11.4.1)* for information about how to export PST files from Outlook. A user can access this section only if he is allowed in Secure User Manager. Please refer to section 6.1.2 (*Secure User Manager*) for information about how to allow users to access this feature.

Using the *Bayesian Classifier* can greatly increase the effectiveness of the spam scanning system. This new functionality allows end-users to upload spam and ham as PST files and makes maintenance of the Bayes database much easier. The more up-to-date the Bayes database is, the less spam you will receive. If there is spam mail that the filter missed, that mail can be learned in this section so that the filter will be able to classify further mail correctly.

It is important to note that the *Bayesian Classifier* will not *kick in* until it has learned at least 200 spam and 200 ham messages. Uploading ham is just as important as uploading spam, so the reader is encouraged to upload both as often as possible.



Spam Learning Center can be accessed by clicking on *Spam Learning Center* in the section *Email Settings* from the main screen of the *Secure User Manager*.



Ham PST Filename Click *Browse* and select the PST file containing your legitimate mails (ham).

Spam PST Filename Click *Browse* and select the PST file containing your spam.

Upload Options The *Forget Messages* option allows you to force the filter to forget the mail thatwas erroneously trained previously. If you think you trained the filter using legitimate mail as spam or vice versa, you can retrain those messeges using this option. Checking this box will make the Bayesian database forget those mail if it had learned them before.

Click the *Proceed With Upload* button to upload the mail. You can upload either ham or spam at a time, or upload them both at the same time.

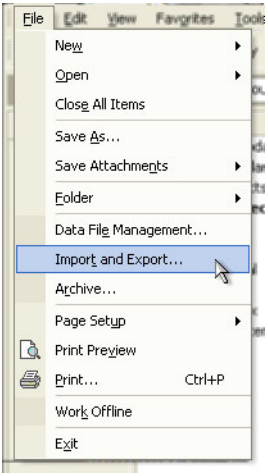
11.6.1 Exporting PST Files From Outlook

Exporting a PST file from Microsoft Outlook is straightforward. Instruct your users to create folders in Microsoft Outlook named "SPAM" and "HAM." These folders must be in all upper-case or the *Secure User Manager* will reject them.

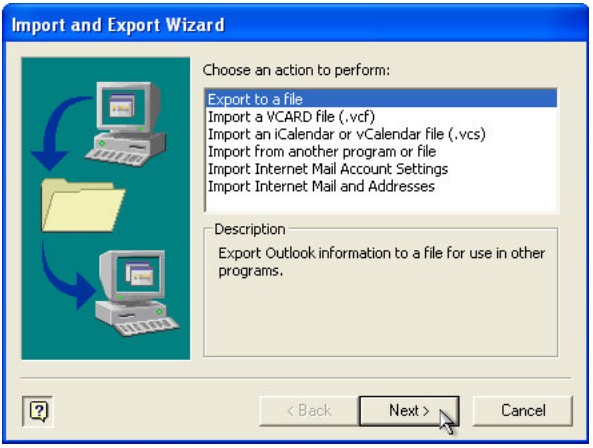
Use the steps below to export SPAM and/or HAM folders to PST files:

- Launch Microsoft Outlook.

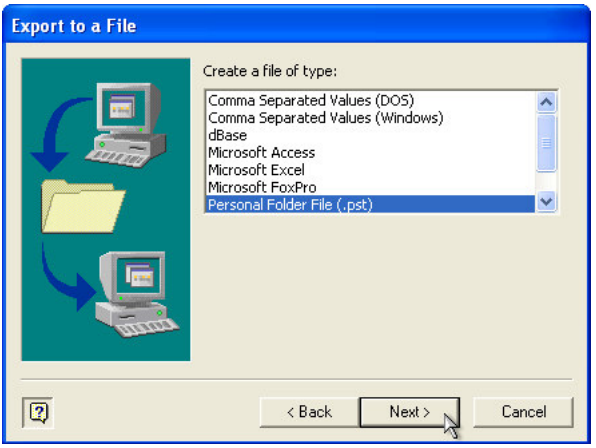
- Go File -> Import and Export...



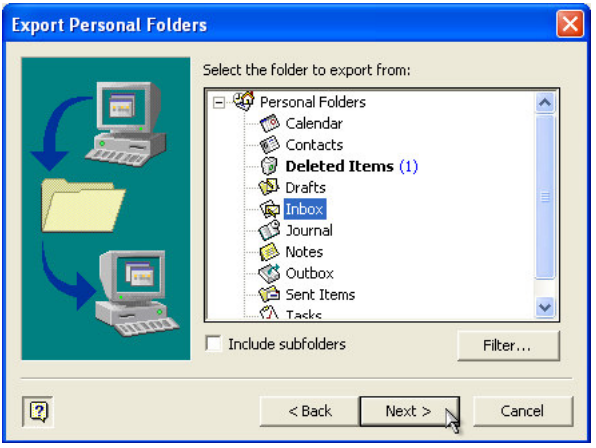
- Select "Export to a file", click "Next >"


Import and Export Wizard
Choose an action to perform:
Export to a File
Import a VCARD file (.vcf)
Import an iCalendar or vCalendar file (.vcs)
Import from another program or file
Import Internet Mail Account Settings
Import Internet Mail and Addresses
Description
Export Outlook information to a file for use in other programs.
< Back
Next >
Cancel

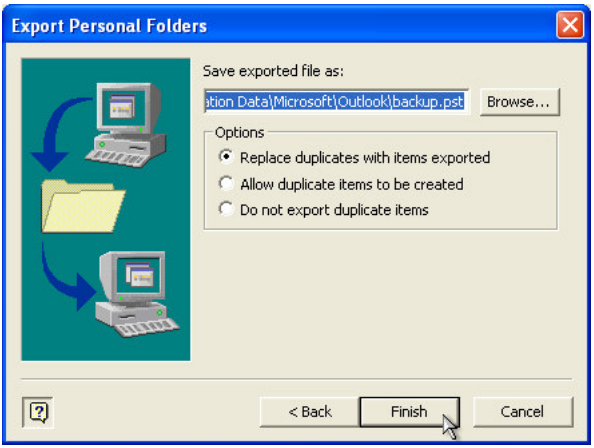
- Select "Personal Folder File (.pst)", click "Next >"



- Select the folder that you want to export, click "Next >"



- Select the location where you want the file saved.



- Give the file a name and check off "No Encryption"

- Finally click "OK".

Do this for each SPAM and HAM folder you have configured in Outlook. When you are done you must quit Outlook.

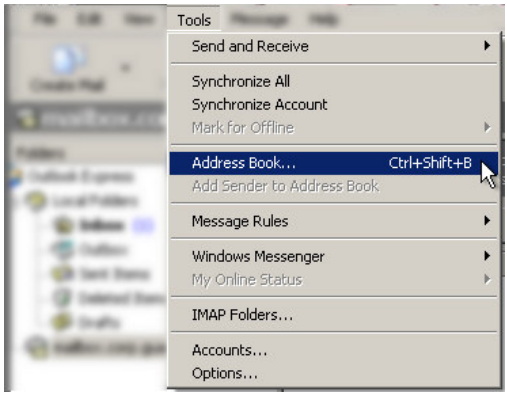
It is also recommended that you clear your HAM and SPAM folders after each import. The *Secure Mail Suite* can recognize and skip duplicate messages, but importing will be much faster if there are no duplicates.

12 Address Books and E-Mail Client Configuration

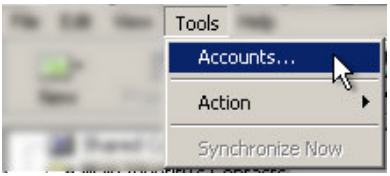
12.1 Outlook Express 6

1. Start *Outlook Express 6* from the *Start Menu*.

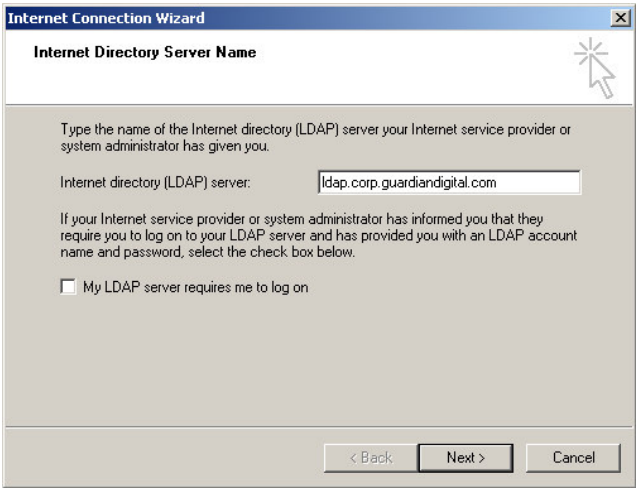
2. Open the *Address Book* by selecting *Address Book* from the *Tools* menu on the toolbar.



3. From the *Address Book* menu select *Tools* from the toolbar and click *Accounts*.

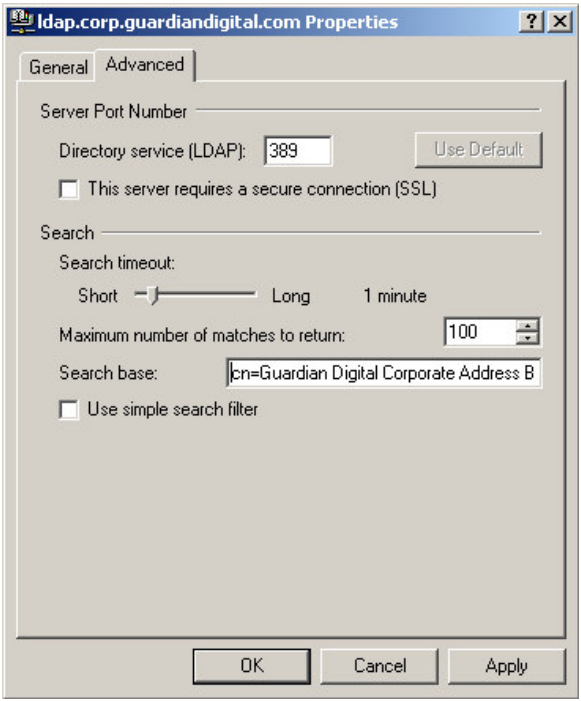


4. The *Internet Accounts* window will appear. Select *Add...* from here.


Internet Connection Wizard
Internet Directory Server Name
Type the name of the Internet directory (LDAP) server your Internet service provider or system administrator has given you.
Internet directory (LDAP) server:
ldap.corp.guardiandigital.com
If your Internet service provider or system administrator has informed you that they require you to log on to your LDAP server and has provided you with an LDAP account name and password, select the check box below.
My LDAP server requires me to log on
< Back
Next >
Cancel

5. Enter in the hostname of the LDAP server in the *Internet directory (LDAP) server* box.

6. Click the *Advanced* tab.

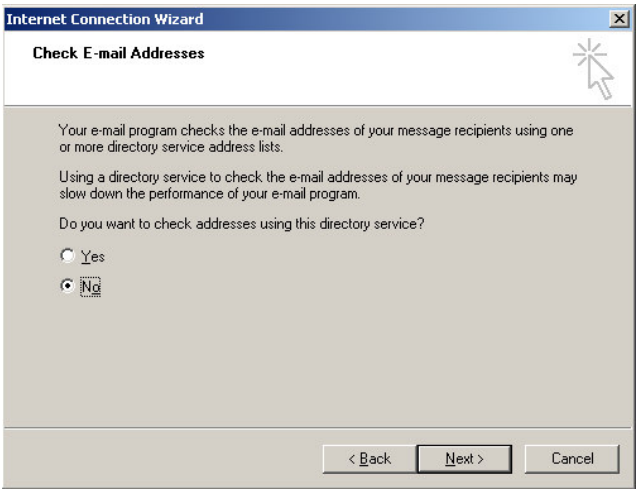


7. Fill in the *Search Base*. The *Search Base* will be the name of the address book, followed up by the standard structure used for address books in the *Secure Mail Suite*.

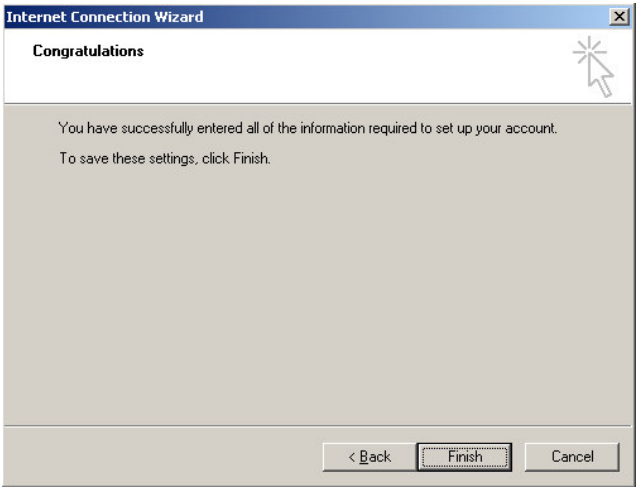
   For example, if the name of the address book is *Guardian Digital Corporate Address Book* and the domain the LDAP server is configured for is set to *dc=corp, dc=guardiandigital,dc=com* then the *Search Base* would be as follows:

   ```
   cn=Guardian Digital Corporate Address Book,cn=address_books,
   ou=public_services,dc=corp,dc=guardiandigital,dc=com
   ```

8. Click *Next* to continue.


Internet Connection Wizard
Check E-mail Addresses
Your e-mail program checks the e-mail addresses of your message recipients using one or more directory service address lists.
Using a directory service to check the e-mail addresses of your message recipients may slow down the performance of your e-mail program.
Do you want to check addresses using this directory service?
Yes
No
< Back
Next >
Cancel

9. Make certain the *No* button is selected and click *Next*.

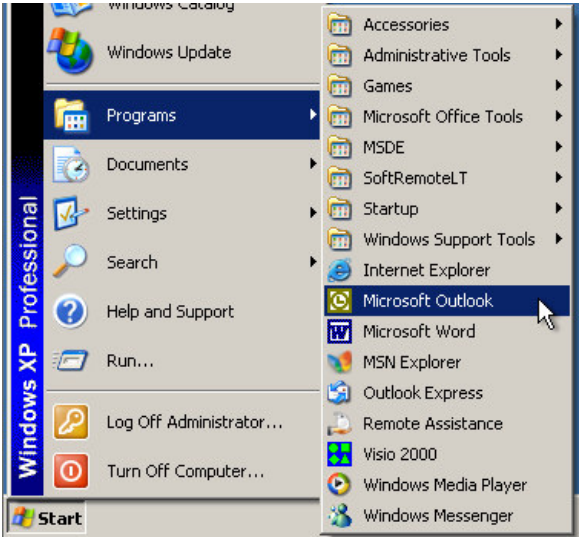

Internet Connection Wizard
Congratulations
You have successfully entered all of the information required to set up your account.
To save these settings, click Finish.
< Back
Finish
Cancel

10. A confirmation screen will appear, click *Finish*.
11. The LDAP server will appear in the list of servers. Click *Close*.

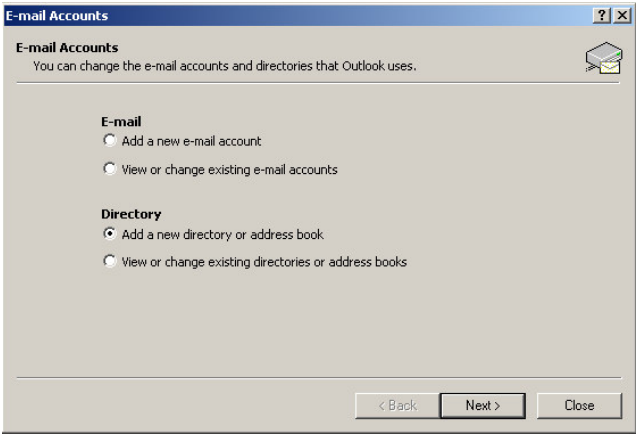
12. At this point it is configured. The *Find People* option can be used and the LDAP server selected from the pull-down menu.

12.2 Outlook XP

1. Start *Outlook XP* from either the desktop icon, if it exists or from the *Start Menu*.

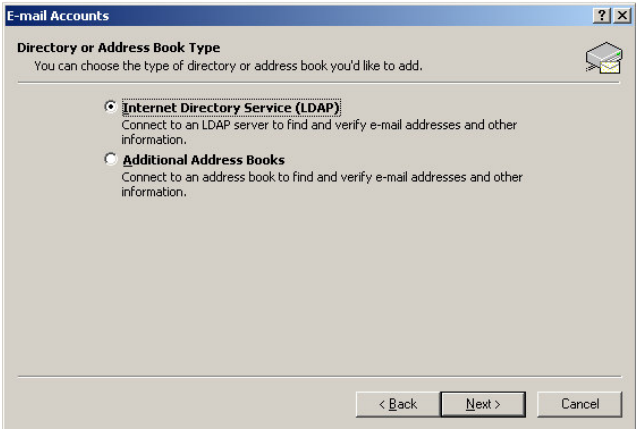


2. From the tool-bar select *Tools* and then *E-Mail Accounts*.


E-mail Accounts
E-mail Accounts
You can change the e-mail accounts and directories that Outlook uses.
E-mail
Add a new e-mail account
View or change existing e-mail accounts
Directory
Add a new directory or address book
View or change existing directories or address books
< Back
Next >
Close

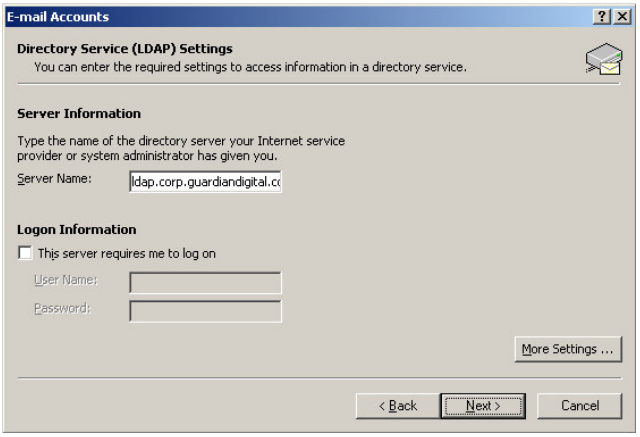
3. The *E-Mail Accounts* wizard will start at this point. From the first menus select *Add* a new directory or address book.

4. Click *Next*.

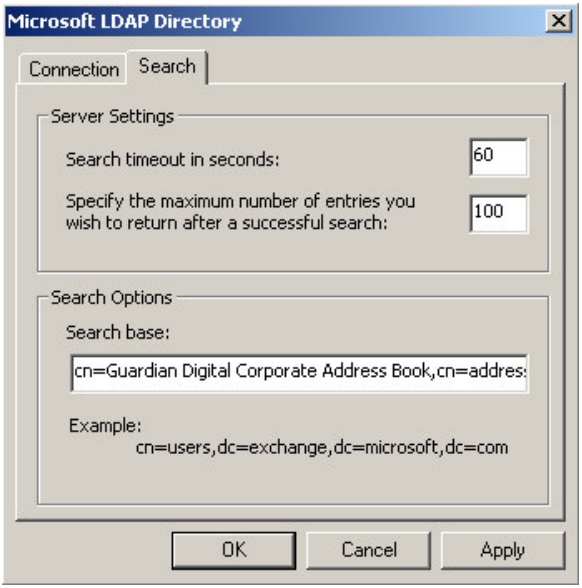

E-mail Accounts
Directory or Address Book Type
You can choose the type of directory or address book you'd like to add.
Internet Directory Service (LDAP)
Connect to an LDAP server to find and verify e-mail addresses and other information.
Additional Address Books
Connect to an address book to find and verify e-mail addresses and other information.
< Back
Next >
Cancel

5. Select *Internet Directory Service (LDAP)*.

6. Click *Next*.


E-mail Accounts
Directory Service (LDAP) Settings
You can enter the required settings to access information in a directory service.
Server Information
Type the name of the directory server your Internet service provider or system administrator has given you.
Server Name:
ldap.corp.guardiandigital.c
Logon Information
This server requires me to log on
User Name:
Password:
More Settings ...
< Back
Next >
Cancel

7. Enter the hostname of the LDAP server in the *Server Name* field.
8. Click the *More Settings* button.
9. From the Microsoft LDAP Directory window click the Search tab.



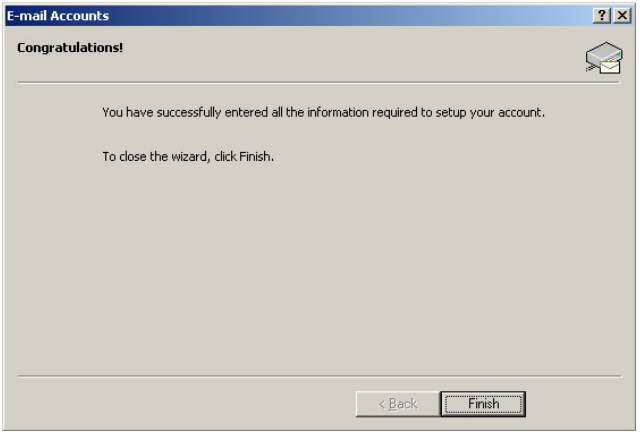
10. Fill in the *Search Base*. The *Search Base* will be the name of the address book, followed up by the standard structure used for address books in the *Secure Mail Suite*.

    For example, if the name of the address book is *Guardian Digital Corporate Address Book* and the domain the LDAP server is configured for is set to *dc=corp, dc=guardiandigital,dc=com* then the *Search Base* would be as follows:

```
cn=Guardian Digital Corporate Address Book,cn=address_books,
ou=public_services,dc=corp,dc=guardiandigital,dc=com
```

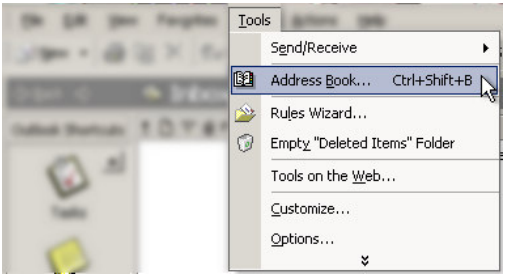
11. Click *OK*.

12. Click *Next* to continue.


E-mail Accounts
Congratulations!
You have successfully entered all the information required to setup your account.
To close the wizard, click Finish.
< Back
Finish

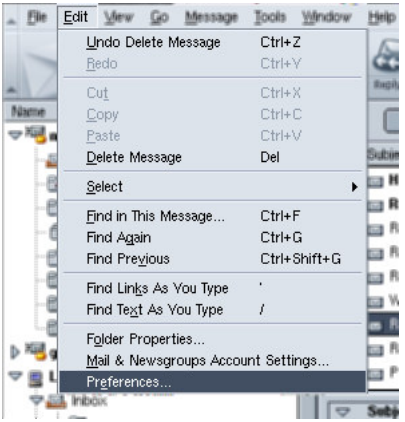
13. A confirmation window will appear. Click *Finish*.

14. To access the address book, from the tool-bar select *Tools* and then *Address Book*.

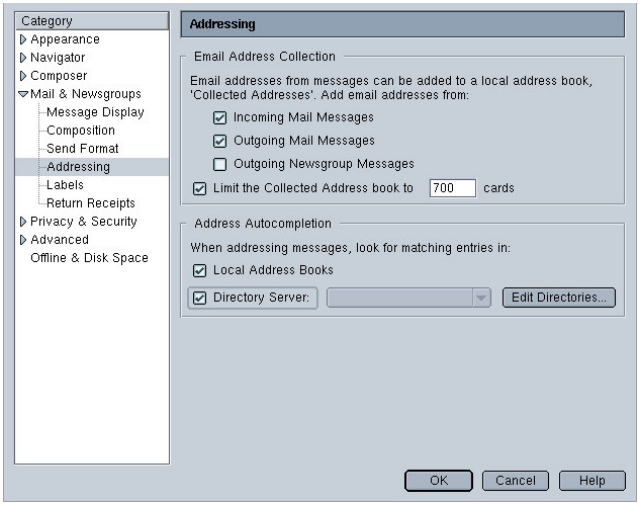


12.3 Netscape Messenger 7

1. Start Netscape Messenger
2. From the *Edit* menu found on the tool-bar select *Preferences*.

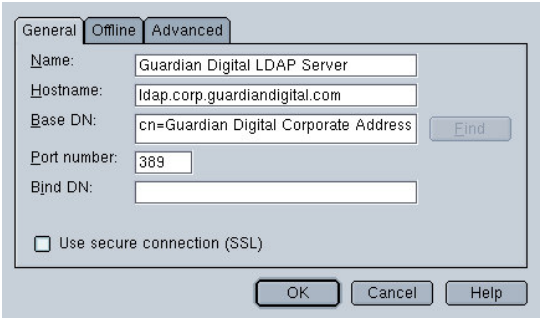


3. From the left side pull-down tree, select *Addressing*.
4. The menu on the right will change. Check *Directory Server*.
5. Click *Edit Directories*.



6. Click *Add* in the *LDAP Directory Servers* window.

7. The *Directory Server Properties* windows will appear after clicking *Add*. In the *General* tab the following fields must be completed:



(a) The *Name* field requires a name to be assigned to this directory service. This is used only as a visual reference.

(b) The *Hostname* is the actual hostname of the LDAP server.

(c) The *Base DN* is the top level DN that will be used when accessing the address book. The *Base DN* will be the name of the address book, followed up by the standard structure used for address books in the *Secure Mail Suite*.

For example, if the name of the address book is *Guardian Digital Corporate Address Book* and the domain the LDAP server is configured for is set to *dc=corp, dc=guardiandigital,dc=com* then the *Base DN* would be as follows:

```
cn=Guardian Digital Corporate Address Book,cn=address_books,
ou=public_services,dc=corp,dc=guardiandigital,dc=com
```

8. Make certain the *Port Number* is set to 389, the *Bind DN* is empty and *Use Secure Connection* (SSL) has not been selected.

9. Click *OK*.

10. You will be returned to the *LDAP Directory Servers* window. Click *OK*.

11. The server is now configured. Click *OK* to exit the *Preferences* window.

12. Now when the address book feature of Netscape Messenger is used it will automatically reference the LDAP server for address book entries.

13 Configuring the E-Mail Client for TLS

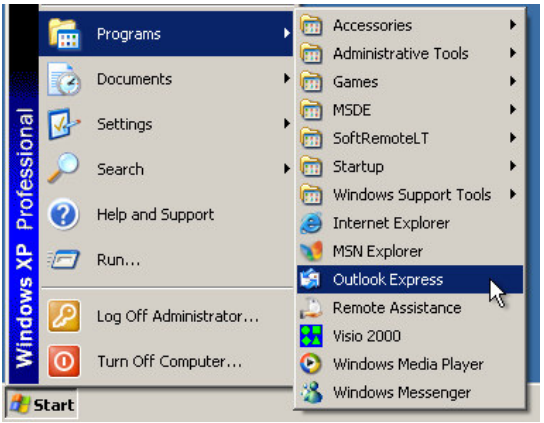
13.1 Outlook Express 6

Outlook Express 6, included with Windows XP supports TLS on the EnGarde server. However, it does not make use of a *User Certificate*, so one is not required to be created for Outlook users. Since no *User Certificate* is required *PPP before SMTP* must be enabled, refer to page *9* for information regarding this.

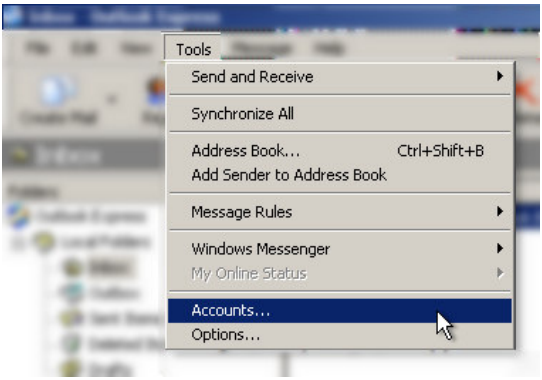
13.1.1 Creating a New E-Mail Account

To setup TLS a user account must be created in Outlook, if an account exists skip to *Configuring E-Mail Accounts for TLS* on page *124*.

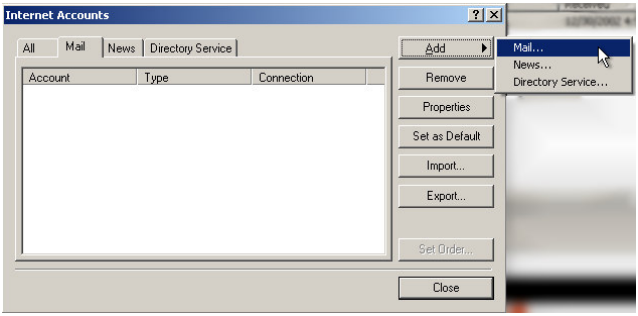
1. From the Windows XP *Start Menu* select *Programs* and then *Outlook Express*.



2. From the Outlook Express Toolbar select *Tools* and then *Accounts...*.



3. The *Internet Accounts* window will appear. From this menu click *Add* and from the pop-up menu click *Mail*.

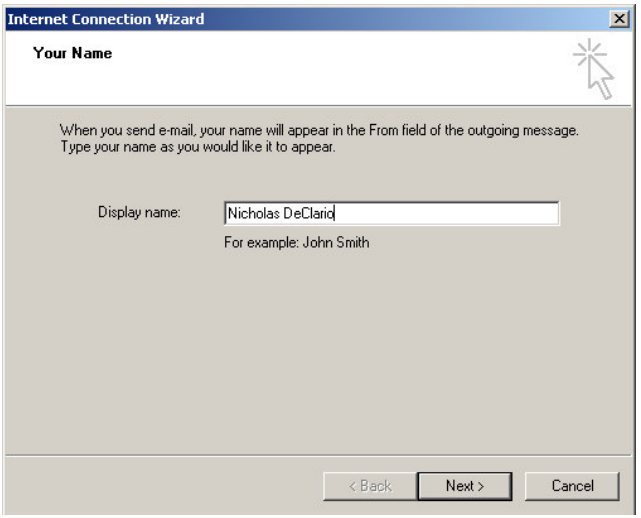


The *Internet Connection Wizard* will start.

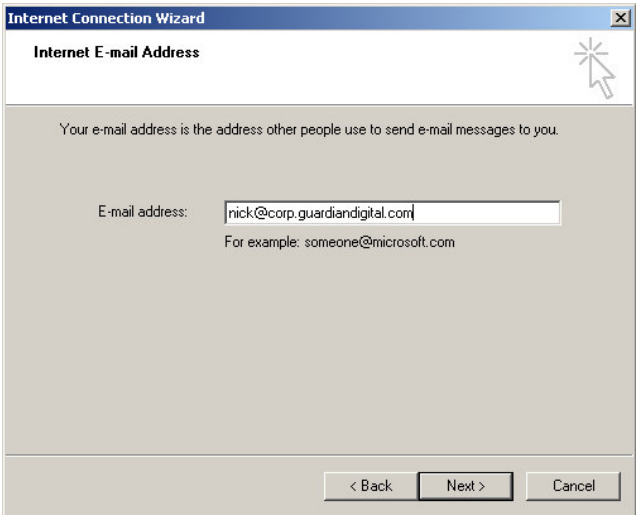
4. Enter in your *Display* name.

   This is the name that will be displayed when an e-mail is sent and received.

5. Once the name has been entered click *Next* to continue.


Internet Connection Wizard
Your Name
When you send e-mail, your name will appear in the From field of the outgoing message.
Type your name as you would like it to appear.
Display name:
Nicholas DeClario
For example: John Smith
< Back
Next >
Cancel

6. In the *E-mail address* entry box enter in the assigned e-mail address.
7. Click *Next* to continue.


Internet Connection Wizard
Internet E-mail Address
Your e-mail address is the address other people use to send e-mail messages to you.
E-mail address:
nick@corp.guardiandigital.com
For example: someone@microsoft.com
< Back
Next >
Cancel

8. Choose the incoming mail server, either *POP* or *IMAP* from the pull-down menu.

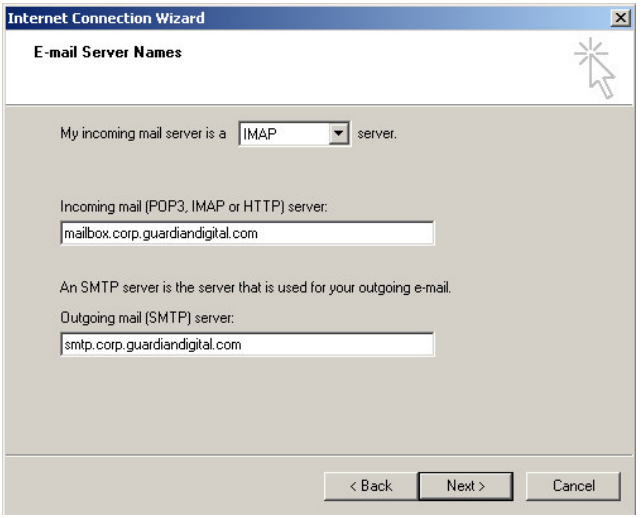
9. In the *Incoming mail (POP3, IMAP, HTTP) server* box enter the mail server that holds the mail.

   Using the example in this manual, mail is stored on *mailbox.corp.guardiandigital.com*. So that is what would be entered in here.

10. Fill in the appropriate outgoing mail server (SMTP) in the *Outgoing mail (SMTP)* server box.

    In the example used, *smtp.corp.guardiandigital.com* is the mail relay that receives all incoming mail for the domain.

11. Click *Next* to continue.

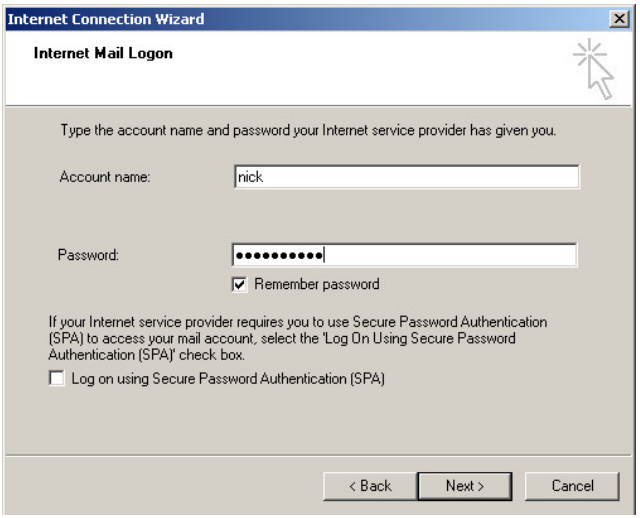


12. Next enter the account name in the *Account name* field. This is the user name assigned to the user.

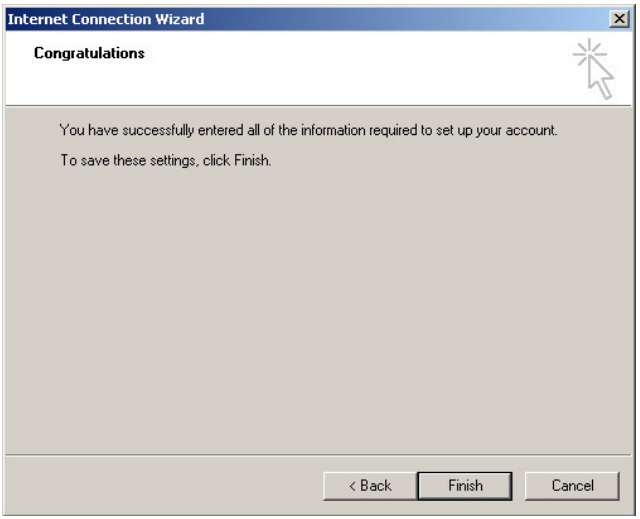
13. Then enter the users password into the *Password* field.

14. Check to make certain that the check-box for *Log on using Secure Password Authentication (SPA)* is ***not*** checked.

15. Click *Next* to continue.


Internet Connection Wizard
Internet Mail Logon
Type the account name and password your Internet service provider has given you.
Account name:
nick
Password:
Remember password
If your Internet service provider requires you to use Secure Password Authentication (SPA) to access your mail account, select the 'Log On Using Secure Password Authentication (SPA)' check box.
Log on using Secure Password Authentication (SPA)
< Back
Next >
Cancel

16. The final screen will appear in the account creation. Click *Finish* to complete the new account creation.

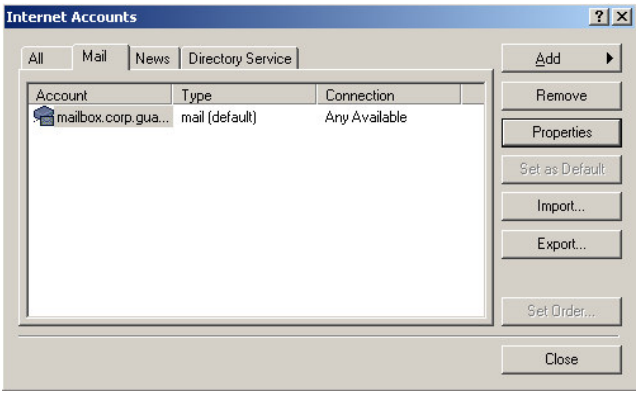

Internet Connection Wizard
Congratulations
You have successfully entered all of the information required to set up your account.
To save these settings, click Finish.
< Back
Finish
Cancel

17. After clicking *Finish* you will be returned to the *Internet Accounts* window.

13.1.2 Configuring E-Mail Accounts for TLS

1. From the *Internet Accounts* windows click on the e-mail account that TLS needs to be configured for and click *Add*.

   NOTE: If no e-mail account exists refer to the previous section *Creating an E-Mail Account* on page *118*.



   A new window will appear with the title of the mail server account.

2. Select the *Servers* tab.

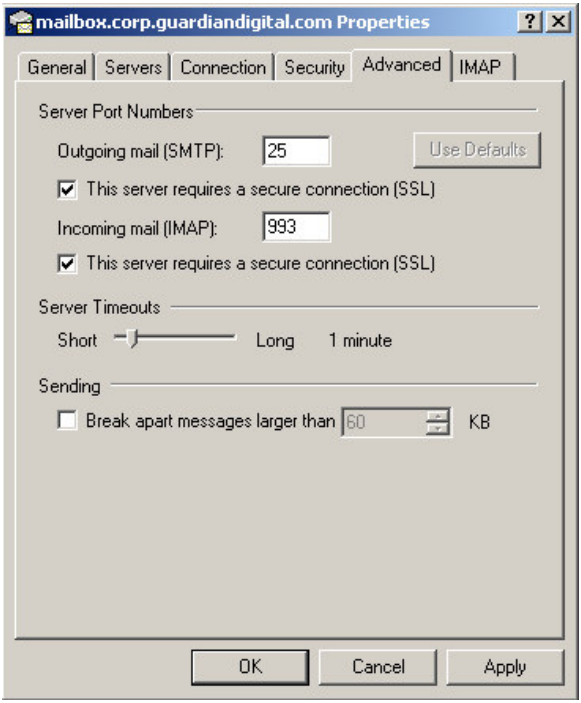
   (a) Make certain *Log on using Secure Password Authentication* is not selected.

   (b) Check *My server requires authentication* check-box.

   (c) Click the *Settings...* button.

3. From the *Outgoing Mail Server* screen select the *Log on Using* radio button.
4. Enter the *Account name* and *Password*. These are the same as used when creating the account for the incoming mail server.
5. Check that *Log on using Secure Password Authentication* is ***not*** set.
6. Click *OK* to continue

7. Back at the *Properties* window select the *Advanced* tab.
8. Check *This server requires a secure connection (SSL)* below for both *Outgoing mail (SMTP)* and *Incoming mail (IMAP).*
9. Click *OK*.



10. Back at the *Internet Accounts* window click *Close*.

E-Mail can now be sent and received via a TLS secured connection.

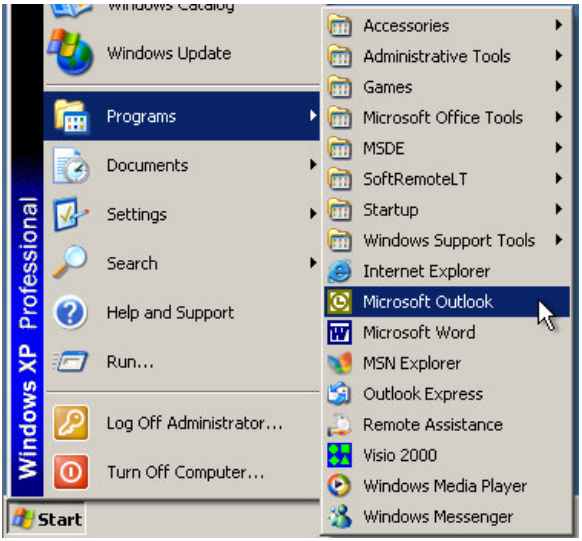
NOTE: Outlook will prompt you if you wish to use a user with an certificate signed by a non-valid Certificate Authority. Accept the prompt and continue as normal.

13.2 Outlook XP

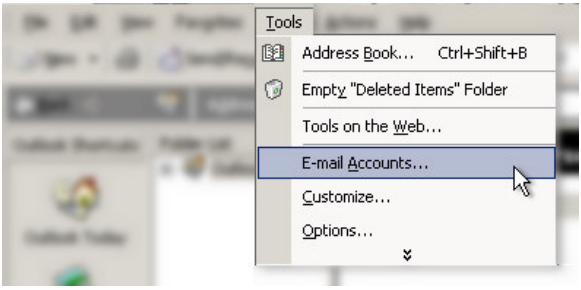
Outlook XP, included with Office XP supports TLS on the EnGarde server. However, as with Outlook Express, it does not make use of a *User Certificate*, so one is not required to be created for Outlook users. Since no *User Certificate* is required *PPP before SMTP* must be enabled, refer to page 9 for information regarding this.

13.2.1 Creating a new TLS Enabled Account

1. Start Microsoft Outlook XP by clicking *Start*, then *Programs* and *Microsoft Outlook*.

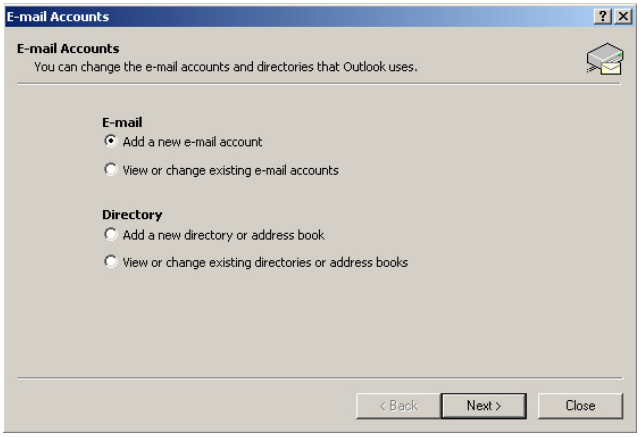


2. Once Outlook has loaded select *Tools* from the toolbar and click E-*mail Accounts....*



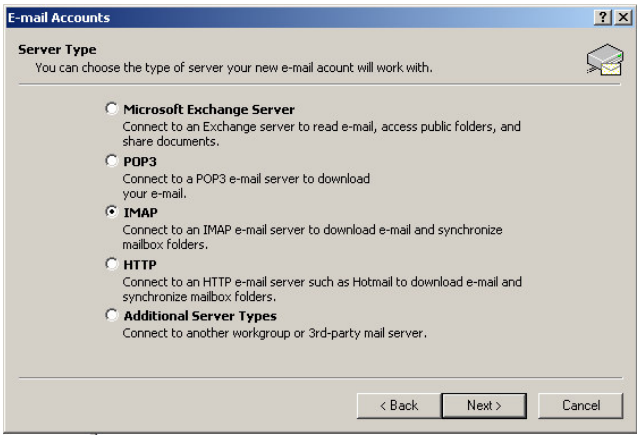
3. The *E-mail Accounts* window will now appear. From this window select the *Add a new e-mail account* radio button. Make certain nothing else is selected.

4. Click *Next* to continue.


E-mail Accounts
E-mail Accounts
You can change the e-mail accounts and directories that Outlook uses.
E-mail
Add a new e-mail account
View or change existing e-mail accounts
Directory
Add a new directory or address book
View or change existing directories or address books
< Back
Next >
Close

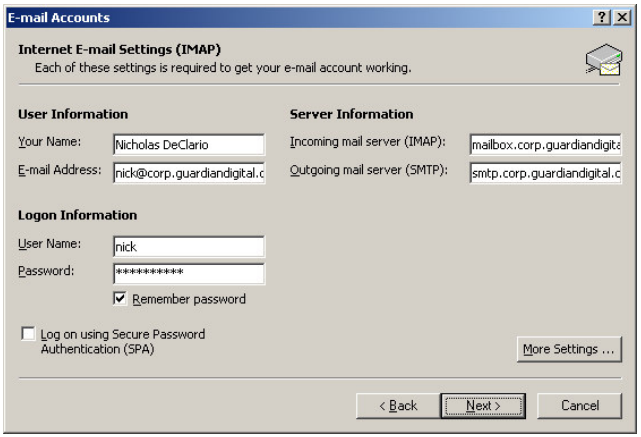
5. Next choose either *POP3* or *IMAP*. The other options here will not work with the *Secure Mail Suite*.

6. Click *Next* to continue.


E-mail Accounts
Server Type
You can choose the type of server your new e-mail acount will work with.
Microsoft Exchange Server
Connect to an Exchange server to read e-mail, access public folders, and share documents.
POP3
Connect to a POP3 e-mail server to download your e-mail.
IMAP
Connect to an IMAP e-mail server to download e-mail and synchronize mailbox folders.
HTTP
Connect to an HTTP e-mail server such as Hotmail to download e-mail and synchronize mailbox folders.
Additional Server Types
Connect to another workgroup or 3rd-party mail server.
< Back
Next >
Cancel

Now the main account information needs to be configured.

7. Configure each item as follows:



(a) *Your Name* is the name that will be displayed when e-mail is sent and received.

(b) In the *E-mail Address* entry box enter in the assigned e-mail address.

(c) In the *Incoming mail server (IMAP)* box enter the mail server that holds the e-mail.

Using the example in this manual, mail is stored on *mailbox.corp.guardiandigital.com*. So *mailbox.corp.guardiandigital.com* would be entered here.

(d) Fill in the appropriate outgoing mail server, the SMTP server in the *Outgoing mail server (SMTP)* server box.

In the example used, *smtp.corp.guardiandigital.com* is the mail relay that receives all incoming mail for the domain.

(e) Enter the *User Name* in this field. This is the user name assigned to the user when the account in the *Secure Mail Suite* was created.

(f) Enter the users password into the *Password* field.

(g) *Log on using Secure Password Authentication (SPA)* should ***not*** be checked

8. When done click *More Settings*.

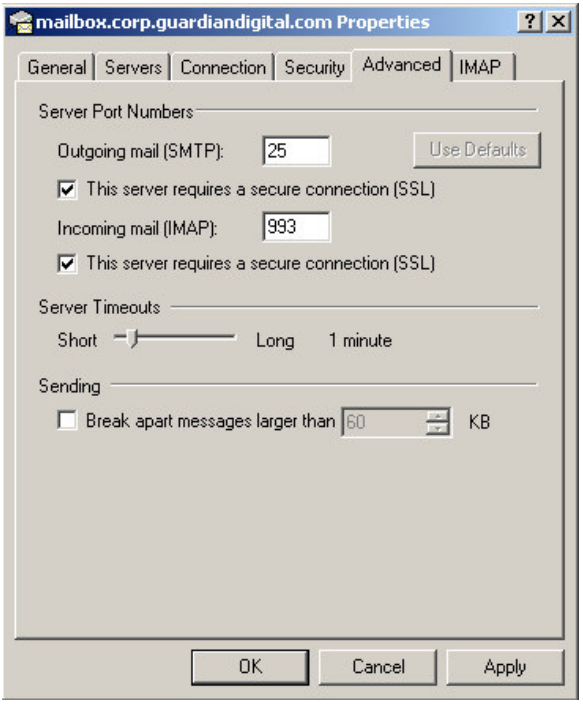
9. The *Internet E-Mail Settings* will open at this point. Select the *Outgoing Server* tab.

10. The fields will be grayed out until the *My outgoing server (SMTP) require authentication* check-box has been checked, check it.

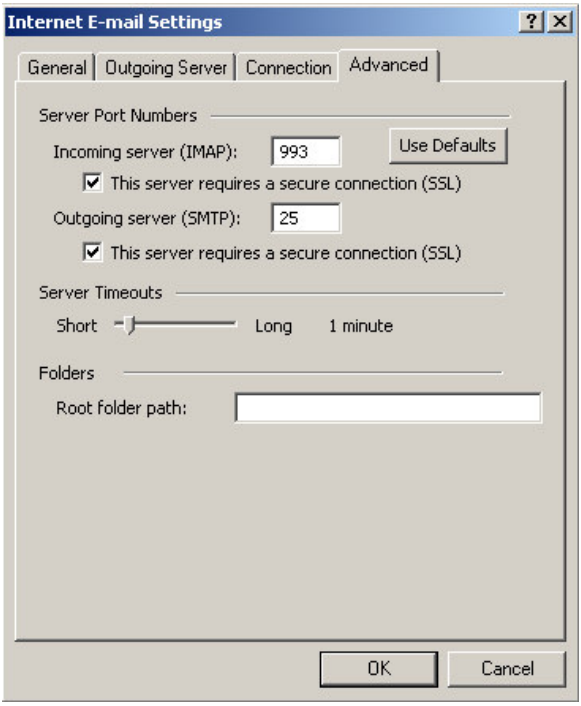
11. Select the *Log on using* radio button which will allow the *User Name* and *Password* fields to be active.

    Fill in both fields with the same information as used in the previous steps.

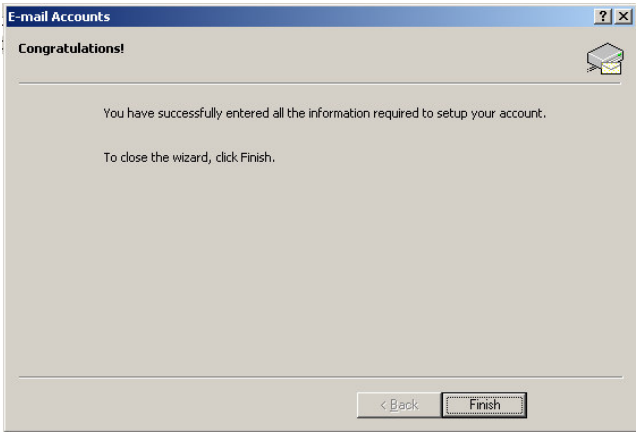
12. Make certain *Log on using Secure Password Authentication* is ***not*** selected.



13. Click the *Advanced* tab
14. Check the *This server requires a secure connection (SSL)* for both the *Incoming server (IMAP)* and *Outgoing server (SMTP)*.
15. Click *OK*.



16. Back at the *E-Mail Accounts* window click the *Next* button.

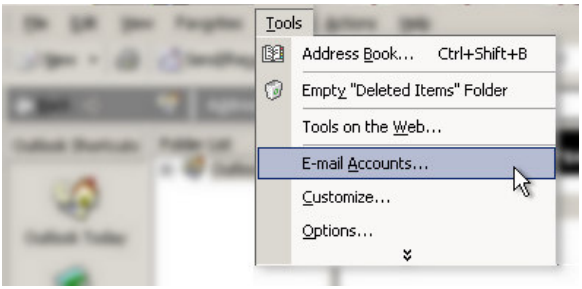

E-mail Accounts
Congratulations!
You have successfully entered all the information required to setup your account.
To close the wizard, click Finish.
< Back
Finish

17. A confirmation screen will appear. Click *Finish* to complete the process.

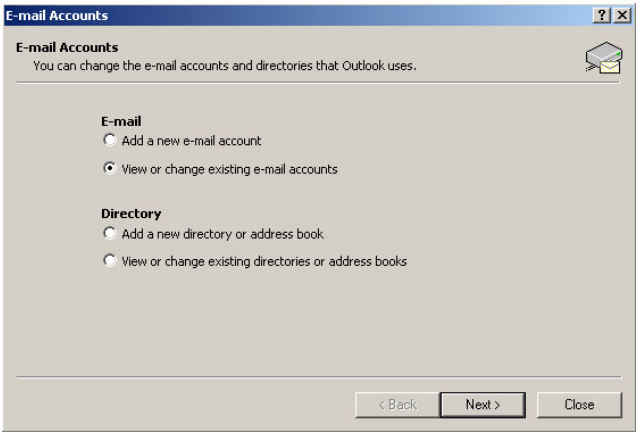
13.2.2 Enabling TLS on an Existing Account

If there is a valid account already in place in Outlook that only needs to have TLS enabled, follow these steps.

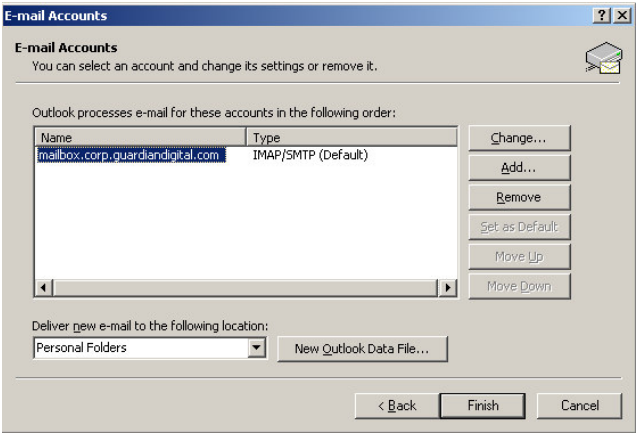
1. From the main Outlook toolbar select *Tools* and then *E-Mail Accounts...*.



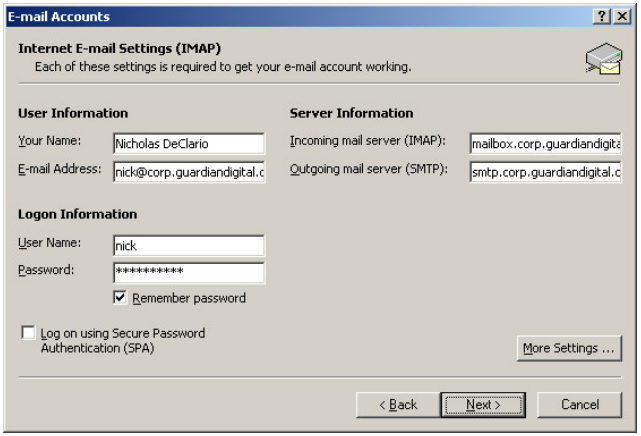
2. From the *E-Mail Accounts* window that opens up select *View* or change existing e-mail accounts and click *Next*.


E-mail Accounts
E-mail Accounts
You can change the e-mail accounts and directories that Outlook uses.
E-mail
Add a new e-mail account
View or change existing e-mail accounts
Directory
Add a new directory or address book
View or change existing directories or address books
< Back
Next >
Close

3. In the next window choose the e-mail address that TLS will be enabled on and click *Change*.



4. Click the *More Settings* button.



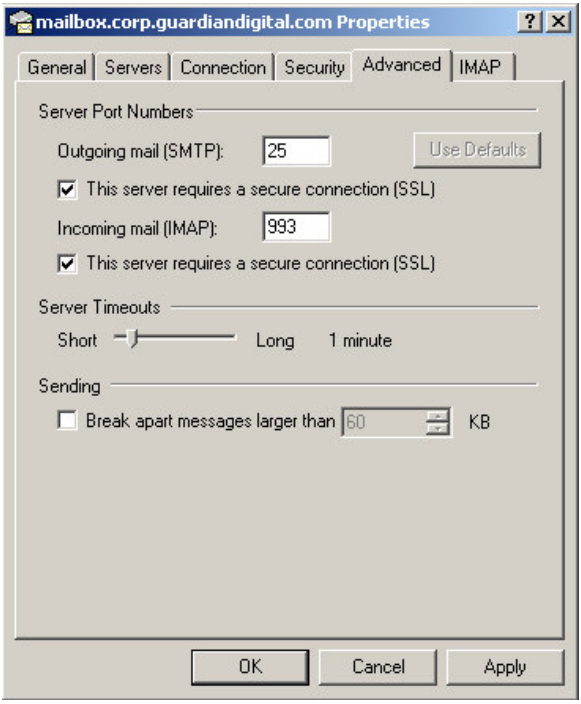
The *Internet E-Mail Settings* will open at this point. Select the *Outgoing Server* tab.

5. The fields will be grayed out until the *My outgoing server (SMTP) require authentication* check-box has been checked, check it.

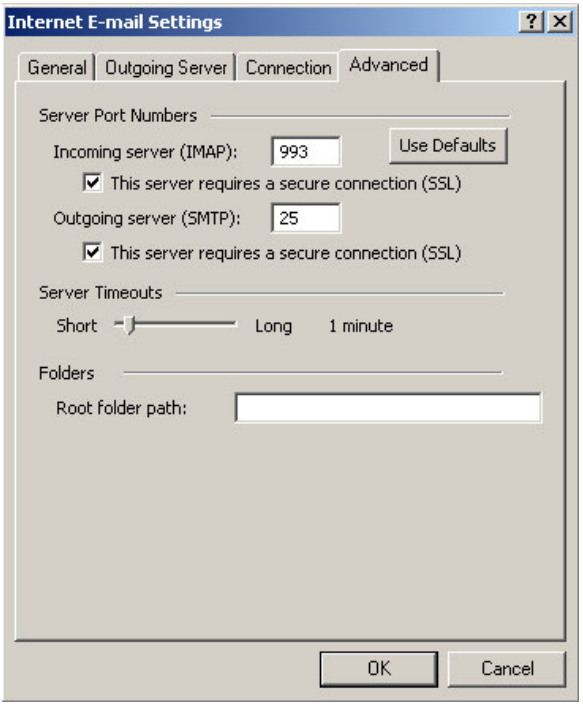
6. Select the *Log on using* radio button which will allow the *User Name* and *Password* fields to be active.

   Fill in both fields with the same information as used in the previous steps.

7. Make certain *Log on using Secure Password Authentication* is ***not*** selected.



8. Click the *Advanced* tab
9. Check the *This server requires a secure connection (SSL)* for both the *Incoming server (IMAP)* and *Outgoing server (SMTP)*.
10. Click *OK*.



11. Back at the *E-Mail Accounts* window click the *Next* button.
12. Click *Finish*.

13.3 Netscape Messenger 7

13.3.1 Creating a New E-Mail Account

To setup an e-mail account in Netscape Messenger with TLS follow the following steps.

This process starts with a new account, if an account already exists skip to step 4.

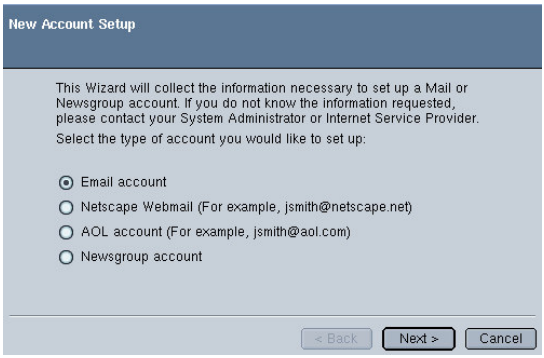
If there are no existing accounts in Netscape or this is a fresh install you will be prompted to create a new account automatically and steps 1 and 2 can be skipped.

1. From the *Netscape Navigator* or *Messenger* window select *Edit* from the tool-bar and then *Mail & Newsgroups Account Settings.*

2. The *Mail & Newsgroups Account Settings* menu will appear. From this menu click the *Add Account...* button.

3. The *Account Wizard* will now appear.

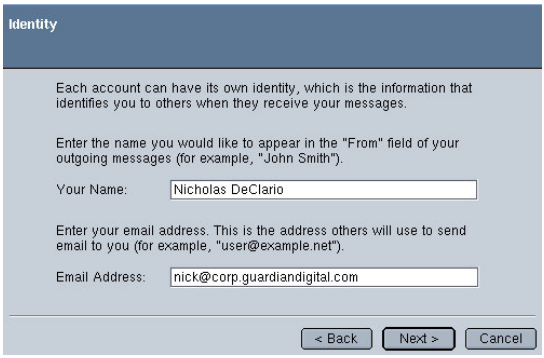
(a) There are several radio buttons in this menu, choose *Email account* and then click *Next* to continue.


New Account Setup
This Wizard will collect the information necessary to set up a Mail or Newsgroup account. If you do not know the information requested, please contact your System Administrator or Internet Service Provider.
Select the type of account you would like to set up:
Email account
Netscape Webmail (For example, jsmith@netscape.net)
AOL account (For example, jsmith@aol.com)
Newsgroup account
< Back
Next >
Cancel

(b) Now the *Your Name* field must be filled in. This is the name that will be displayed in the sender portion of an e-mail when one is sent.

(c) Fill in the *Email Address* with assigned address.

(d) Click *Next* to proceed.


Identity
Each account can have its own identity, which is the information that identifies you to others when they receive your messages.
Enter the name you would like to appear in the "From" field of your outgoing messages (for example, "John Smith").
Your Name:
Nicholas DeClario
Enter your email address. This is the address others will use to send email to you (for example, "user@example.net").
Email Address:
nick@corp.guardiandigital.com
< Back
Next >
Cancel

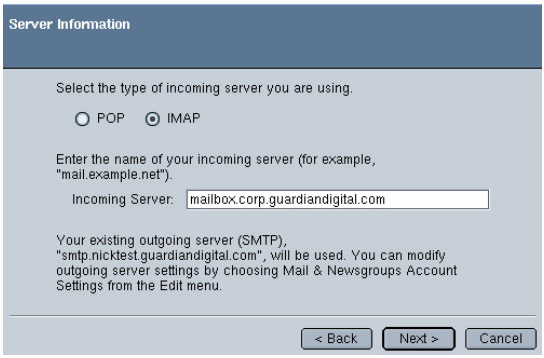
(e) The *Server Information* is now required. Choose between *POP* and *IMAP*.

This is mostly a preference or can be determined by a company policy. Section *5 Definitions and Terminology* on page *5* has a listing for both POP and IMAP.

(f) Choose the *Incoming Server*. This will be the server that your e-mail is stored on and will be fetched from.

In our example scenario mail is delivered to *smtp.corp.guardiandigital.com* which relays it to *mailbox.corp.guardiandigital.com*. *mailbox.corp.guardiandigital.com* acts as our spool and stores the e-mail. So *mailbox.corp.guardiandigital.com* would entered for our *Incoming Server*.

(g) Click *Next* to continue.


Server Information
Select the type of incoming server you are using.
POP
IMAP
Enter the name of your incoming server (for example, "mail.example.net").
Incoming Server:
mailbox.corp.guardiandigital.com
Your existing outgoing server (SMTP), "smtp.nicktest.guardiandigital.com", will be used. You can modify outgoing server settings by choosing Mail & Newsgroups Account Settings from the Edit menu.
< Back
Next >
Cancel

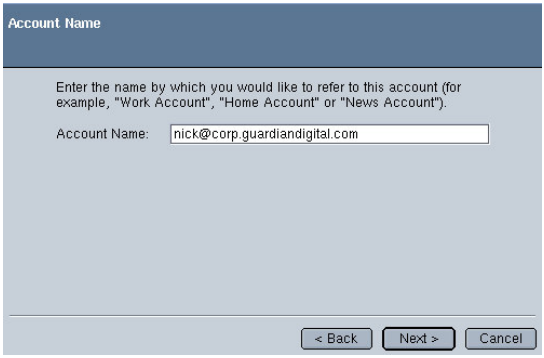
(h) Enter the *User Name* for this account.

When the account was created a user name was assigned to that account. That user would be entered in here.

(i) Click *Next*.

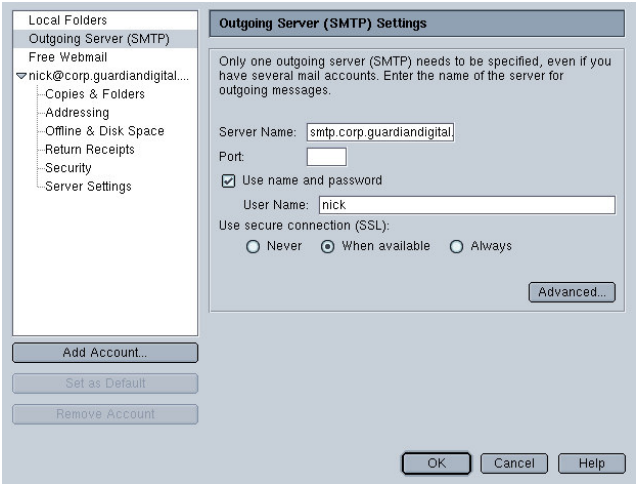
(j) Next the *Account Name* must be configured.
This is simply a display name. It will appear as a reference for this account.

(k) Click *Next* to proceed.


Account Name
Enter the name by which you would like to refer to this account (for example, "Work Account", "Home Account" or "News Account").
Account Name:
nick@corp.guardiandigital.com
< Back
Next >
Cancel

(l) Lastly a confirmation screen will appear. Confirm all the information and click *Finish* to create the account.

4. Returned to the *Mail & Newsgroups Settings* menu select *Outgoing Server (SMTP)* from the left menu. Several new options will appear to the right.



5. The *Server Name* will be the outgoing mail server name. Using the example used in this manual that would be s*mtp.corp.guardiandigital.com.*

   (a) Make certain the *Port* field is blank

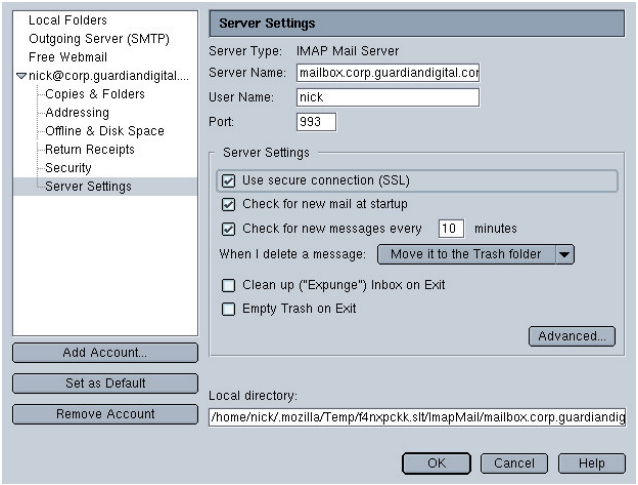
   (b) *Use name and password* must be checked.

   (c) *User Name* should match the user name the user was assigned when their account was created.

   (d) *Use secure connection (SSL)* must be set to *When available*.

6. Next click on the small arrow to the left of the *Account Name*, *nick@corp.guardiandigital.com* in the example used above. This will produce an additional list of options.

7. From this new list select *Server Settings*. A new set of options will appear to the right.



8. Select *Use secure connection (SSL)*.

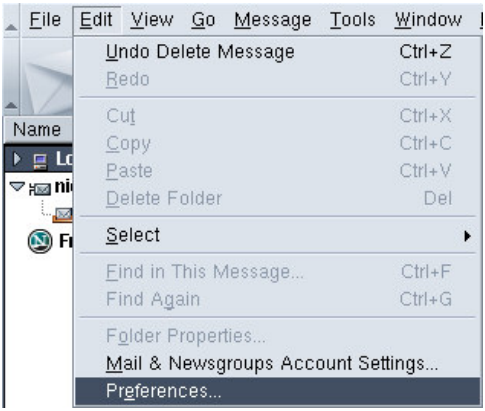
   No other options need to be changed on this menu.

9. Click *OK* to accept the changes.

13.3.2 Import the TLS Certificate

The User Certificate needs to be inserted into Netscape at this point. For information on creating and downloading a *User Certificate* refer to *TLS Server Configuration* section on page *19*.

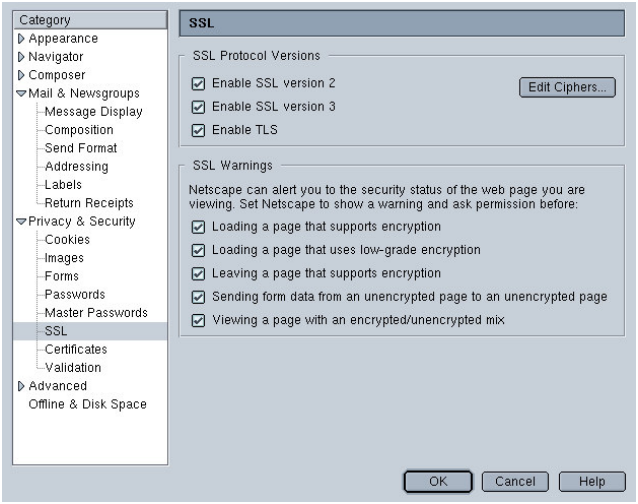
1. From *Netscape Messenger* or *Navigator* select *Edit* and then *Preferences*.



2. From the left side menu click the arrow to the left of *Privacy & Security*. This will drop-down more options.

3. Select *SSL*.

   (a) Make certain *Enable SSL Version 2*, *Enable SSL Version 3* and *Enable TLS* are all selected.

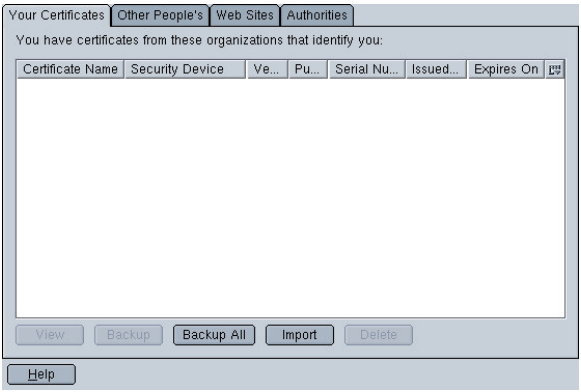


4. From the left side drop-down select *Certificates*.

5. Click *Manage Certificates* on the right side.

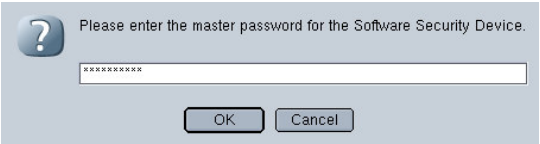
6. Confirm you are currently on the *Your Certificates* tab in the *Certificate Manager* window.

7. Click *Import* from the buttons on the bottom.



8. Choose the location of your user certificate, it will end in *.p12* and hit OK.

9. Netscape will prompt you for the master password to insert/delete certificates. If this is the first time a certificate is being imported into Netscape you will be prompted to create one.

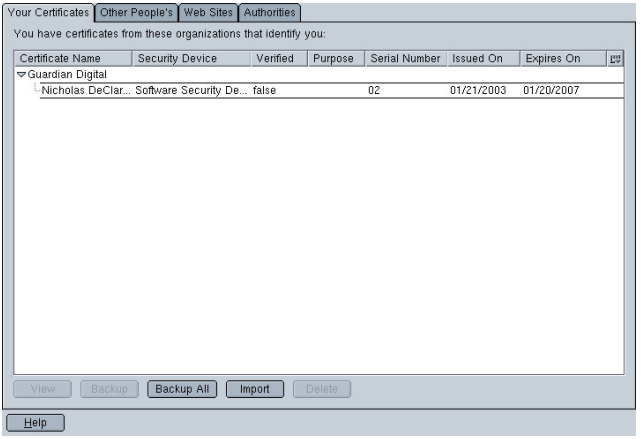


10. Once the password is accepted the password for the certificate itself will be requested. The password here is the e-mail address for the user.

    Using the example in the manual, this would be *nick@corp.guardiandigital.com*.

11. When the password is accepted the certificate will be imported and a message of confirmation will appear.

12. After closing the confirmation the certificate will appear in the *Manage Certificates* window.



13. Close the *Manage Certificates* window.

E-Mail can now be sent over TLS from Netscape.

14 Configuring the E-Mail Client for SPOP and SIMAP

EnGarde Secure Professional provides two methods of retrieving your e-mail remotely, secure IMAP and secure POP3. Both protocols have been secured using SSL and both require clients that support SSL secured IMAP and secured POP3.

Securing IMAP and POP3 greatly increases the security and privacy of personal e-mail. For this reason IMAP and POP3 are only available in a secure form and therefore the standard, insecure form of IMAP and POP3 are not available with EnGarde.

Using a secure form of these protocols requires a client that can support them. We will discuss how to configure both Netscape Mail for secure IMAP, Microsoft Outlook Express and Microsoft Outlook XP for secure IMAP and secure POP3.

14.1 Microsoft Outlook Express

Creating a new account in Outlook Express 6 is covered in the TLS configuration. Follow steps 1 through 17, starting in *section 13.1.1 on page 118*.

14.2 Microsoft Outlook XP

Creating a new account in Outlook XP is covered in the TLS configuration. Follow steps 1 through 17 starting in *section 13.2.1 on page 128*. Skip steps 9 through 12.

14.3 Netscape Messenger 7

Creating a new account in Netscape Messenger is covered in the TLS configuration. Follow steps 1 through 9 starting in *section 13.3.1 on page 138.*

A What is CIDR Notation

Classless Inter Domain Routing (CIDR) is a method for assigning IP addresses without using the standard IP address classes like Class A, Class B or Class C.

In CIDR notation, an IP address is represented as A.B.C.D/n, where "/n" is called the IP prefix or network prefix. The IP prefix identifies the number of significant bits used to identify a network. For example, 192.9.205.22 /18 means, the first 18 bits are used to represent the network and the remaining 14 bits are used to identify hosts. Common prefixes are 8, 16, 24, and 32.

Refer to the following page for the *CIDR to Netmask Translation Table*.

CIDR	Netmask (Dot Notation)	Number of Hosts
/1	128.0.0.0	
/2	192.0.0.0	
/3	224.0.0.0	
/4	240.0.0.0	
/5	248.0.0.0	
/6	252.0.0.0	
/7	254.0.0.0	
/8	255.0.0.0	
/9	255.128.0.0	
/10	255.192.0.0	
/11	255.224.0.0	
/12	255.240.0.0	
/13	255.248.0.0	
/14	255.252.0.0	
/15	255.254.0.0	
/16	255.255.0.0	
/17	255.255.128	
/18	255.255.192.0	
/19	255.255.224.0	
/20	255.255.240.0	
/21	255.255.248.0	
/22	255.255.252.0	
/23	255.255.254.0	
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32
/28	255.255.255.240	16
/29	255.255.255.248	8
/30	255.255.255.252	4
/31	255.255.255.254	2
/32	255.255.255.255	1